Mandriva Linux 2007

DrakXTools User Manual

Mandriva

http://www.mandriva.com

Mandriva Linux 2007: DrakXTools User Manual
Published 2006-09-01
Copyright © 2006 Mandriva SA

by NeoDoc (`http://www.neodoc.biz`)Camille Bégnis, Christian Roy, Fabian Mandelbaum, Roberto Rosselli del Turco, Marco De Vitis, Alice Lafox, John Rye, Wolfgang Bornath, Funda Wang, Patricia Pichardo Bégnis, Debora Rejnharc Mandelbaum, Mickael Scherer, Jean-Michel Dault, Lunas Moon, Céline Harrand, Fred Lepied, Pascal Rigaux, Thierry Vignaud, Giuseppe Ghibò, Stew Benedict, Francine Suzon, Indrek Madedog Triipus, Nicolas Berdugo, Fabrice Facorat, Xiao Ming, Snature , Guylhem Aznar, Pavel Maryanov, Annie Tétrault, Aurelio Marinho Jargas, Felipe Arruda, Marcia Gawlak Hoshi, Roberto Patriarca, Sean Wheller, and Laura Sebrie

Table of Contents

List of Tables

Preface

1. About Mandriva Linux

Mandriva Linux is a GNU/Linux distribution supported by Mandriva S.A. which was born on the Internet in 1998. Its main goal was and still is to provide an easy-to-use and friendly GNU/Linux system. Mandriva's two pillars are open source and collaborative work.

> **Note:** In April 2005 the Mandrakesoft company changed its name to Mandriva to reflect its merger with Brazil-based Connectiva. Its core product, Mandrakelinux, became Mandriva Linux.

1.1. Contacting the Mandriva Linux Community

The following are various Internet links pointing you to the most important Mandriva Linux-related sources. If you wish to know more about the Mandriva company, connect to our web site (`http://www.mandriva.com/`). You can also check out the Mandriva Linux distribution web site (`http://www.mandriva.com/community/`) and all its derivatives.

Mandriva Expert (`http://www.mandrivaexpert.com/`) is Mandriva's support platform. It offers a new experience based on trust and the pleasure of rewarding others for their contributions.

We also invite you to subscribe to the various mailing lists (`http://www.mandriva.com/community/resources/newsgroups`) where the Mandriva Linux community demonstrates its high spirits and keen debates.

Please also remember to connect to our security page (`http://www.mandriva.com/security`). It gathers all security-related material about Mandriva Linux distributions. You will find security and bug advisories, as well as kernel update procedures, the different security-oriented mailing lists which you can join, and Mandriva Online (`https://www.mandrivaonline.com/`). This page is a must for any server administrator or user concerned about security.

1.2. Join the Club!

Mandriva Club is **the** place where users meet to help each other out, exchange valuable information about Mandriva Linux, get informed of the latest Mandriva, Linux and Open Source news. Club subscribers have privileged access to an even wider array of services.

With your Mandriva ID, you have free access to:

- help (forums, chat, Knowledge Base with tutorials, how-tos, tips and tricks)
- news
- more Mandriva- and community-contributed content

As a Club Member, you have exclusive access to :

- 50.000 software packages, including commercial software, drivers, demos...
- super-fast download servers
- official Mandriva Linux documentation
- Mandriva Online Services - Kiosk, Online, Expert and eTraining
- permanent special discounts at Mandriva Store
- ... and much more !

Mandriva Club is where you get the best Mandriva Linux experience, learning from others, teaching others, accessing exclusive features and contributing to the development of Mandriva Linux and Free and Open Source Software in general.

1.3. Subscribing to Mandriva Online

Mandriva offers a very convenient way to keep your system automatically up-to-date, free of bugs and security holes. Visit the Mandriva Online Web site (`https://www.mandrivaonline.com//`) to learn more about this service.

1.4. Purchasing Mandriva Products

Mandriva Linux users may purchase products on-line through the Mandriva Store (`http://store.mandriva.com/`). You will not only find Mandriva Linux software, operating systems and "live" boot CDs (such as Live), but also special subscription offers, support, third-party software and licenses, documentation, GNU/Linux-related books, as well as other Mandriva goodies.

1.5. Mandriva Kiosk

Mandriva Kiosk is a service which provides you with a catalog of the most popular software, be it Free or commercial, for your Mandriva Linux distribution. You'll find new software for all your needs: from the latest version of the OpenOffice.org suite and multimedia applications to the latest KDE and GNOME desktop environments, games and wallpapers.

It's very easy to use with its web-based graphical interface, detailed application descriptions and a smooth one-click install process that will upgrade or extend your system's functionally in a few minutes. Installing new software on your Mandriva Linux distribution has never been easier.

Mandriva Linux 2007 Discovery, Powerpack and Powerpack+ users benefit from 30 days of free access to Kiosk with their free Club trial period. Discover it now at the Kiosk Website (`http://kiosk.mandriva.com`).

The Mandriva Kiosk service is free to all Mandriva Club members and is also available as a stand-alone service through an annual subscription. By subscribing to Kiosk, you're getting:

• access to an easy-to-use web-based catalog of new software - Free and commercial

• packages tested exclusively for Kiosk by Mandriva teams

• packages which seamlessly install on your system

• packages which install with a single mouse click

Enjoy the Kiosk experience!

1.6. Contributing to Mandriva Linux

The skills of the many-talented folks who use Mandriva Linux can be very useful in the making of the Mandriva Linux system:

• **Packaging.** A GNU/Linux system is mainly made of programs found on the Internet. These need to be packaged in order to work together.

• **Programming.** There are many, many projects directly supported by Mandriva: find the one which most appeals to you and offer your help to the main developer(s).

• **Internationalization.** You can help us translate web pages, programs and their respective documentation.

Consult the development projects (`http://www.mandriva.com/en/community/contribute/join`) page to learn more about how you can contribute to the evolution of Mandriva Linux.

2. MCC's Components

The Mandriva Linux Control Center (MCC) enables the system administrator to configure the hardware and the services used by all users in a friendly way.

Access the Mandriva Linux Control Center through the main menu (System+Configuration→Configure Your Computer).

> **Note:** Some of the Mandriva Linux Control Center components are also available from the command line in text mode by running `drakconf`.
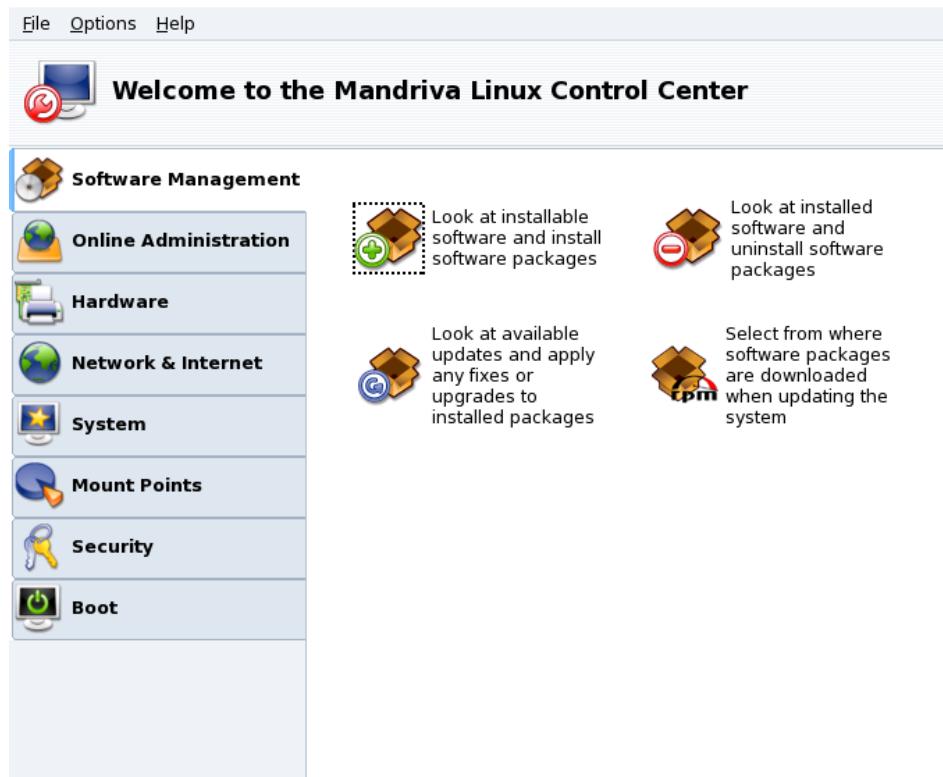
Figure 1. The Control Center's Main Window

Here are some of the available menu entries:

- **Options→Display Logs.** When activated this option displays a Tools Logs window. It shows all system modifications made by the configuration tools launched from within Mandriva Linux Control Center.
- **Options→Expert mode.** Gives you access to some of the more advanced tools, which are shown in the table below.
- **Help→Help.** Opens the help browser which displays documentation about the active configuration tool.
- **Help→Report Bug.** Allows you to report a bug to the development team. See *The Drakbug Reporting Tool*, page 7.

The tools are sorted into categories. The following table lists them all and refers to the corresponding sections of this manual.

Software Management	*"Package Management"*, page 9
	Configuration Uploader: allows you to upload your configuration to the Mandriva Online facility in order to benefit from available software updates. Available only in Mandriva Linux Control Center's expert mode.
Hardware	*Configuring your Hardware*, page 21
	Controlling the Graphical Configuration, page 22
	Configuring the 3D Desktop, page 26
	Setting up a TV Card with DrakxTV, page 27
	Changing your Keyboard Layout, page 28
	Changing your Mouse, page 29
	Configuring Printers with PrinterDrake, page 29
	Installing and Sharing Scanners, page 39
	Setting up your UPS, page 41
Network & Internet	*Network and Internet Connection Management*, page 43
	Proxy Settings, page 50
	Internet Connection Sharing, page 52
	Activating and Managing Network Profiles, page 50
	Wireless Connections Management (Roaming), page 54
	Configure VPN Connections: Allows you to setup a Virtual Private Network with a remote VPN server. Protocols supported are Cisco VPN Concentrator and OpenVPN.
	Manage host definitions: If you have fixed IP addresses on your network, this tool allows you to associate names to those IPs, easier to remember.
System	Menu style configuration: This utility allows you to switch the menu style from the "Discovery" one, to the more complete "Mandriva" one.
	Select the authentication method: This tool allows you to change the way users are authenticated on your computer. Various authentication methods are available. If you select a method other than Local file, you are asked to provide some parameters which vary from one method to the other. If you don't know those parameters, you should ask your network administrator. Available only in Mandriva Linux Control Center's expert mode.
	Display manager chooser: allows you to choose the X11 display manager for users who graphically log onto the machine. Basically, all display managers offer the same features, it's just a question of taste.
	Configuring Start-Up Services, page 57
	Managing Fonts on your System with DrakFont, page 57
	Setting your Machine's Date and Time, page 59
	Select the language and the country or region: This utility allows you to switch the main language of the system, as well as local settings. First choose the language to be used, then the country or region.
	Monitoring System Activity and Status, page 60
	Console: simply opens a terminal to directly enter commands from the administrator account (root).
	Managing Users and Groups, page 63
	Backing Up and Restoring your Files, page 66
Mount Points	*Managing your Hard Drive Partitions with DiskDrake*, page 75

	Managing Removable Devices, page 78
	Importing Remote NFS Directories, page 81
	Manage NFS Shares: Allows you to create and maintain shares to be mounted by other UNIX® machines on the local network.
	Importing Remote SMB Directories, page 79
	Setting up WebDAV Mount Points, page 82. This utility allows you to mount remote WebDAV directories.
	Allowing Users to Share Folders, page 81
	Manage Samba configuration: This tool allows you to manage the folders and printers of your machine shared with Windows® machines on the local network. It also allows you to manage Samba users for shares access control.
Security	*Securing your Machine through DrakSec*, page 85. Available only in Mandriva Linux Control Center's expert mode.
	Controlling File Permissions with DrakPerm, page 87. Available only in Mandriva Linux Control Center's expert mode.
	Securing your Internet Access via DrakFirewall, page 88
	Setup network interfaces failover and firewall replication: mainly useful for clusters, this tool allows you to define redundancy for network interfaces, as well as firewall replication.
Boot	*Configuring the Login Mode*, page 93
	Changing your Boot-up Configuration, page 93
	Customizing your Boot Theme, page 94

Table 1. Overview of Graphical Tools

Note: Additionally, the Online Administration category only appears if the rfbdrake package is installed. This tool allows you to take control of a remote host (Linux/UNIX®, Windows®). We cover the usage Rfbdrake in "*Controlling a Remote Machine*", page 15.

Some other categories appear if the drakwizard package is installed. The documentation for those wizards is available ondisk as well as in the *Server Administration Guide*. Those wizards enable you to do basic configuration of common LAN services such as web, FTP, mail and database servers.

3. Conventions Used in this Book

3.1. Typing Conventions

Formatted Example	Meaning
inode	Used to emphasize a technical term.
`ls -lta`	Used for commands and their arguments. (see *Commands Synopsis*, page 6).
`a_file`	Used for file names. It may also be used for RPM package names.
ls(1)	Reference to a `man` page. To read the page, simply type `man 1 ls`, in a command line.
`$ ls *.pid`	Formatting used for text snapshots of what you may see on your screen including computer interactions, program listings, etc.
`localhost`	Literal data which does not generally fit in any of the previously defined categories. For example, a key word taken from a configuration file.

Formatted Example	Meaning
OpenOffice.org	Defines application names. Depending on context, the application and command name may be the same but formatted differently. For example, most commands are written in lowercase, while applications names usually begin with an uppercase character.
Files	Indicates menu entries or graphical interface labels. The underlined letter, if present, informs you of a keyboard shortcut, accessible by pressing the **Alt** key plus the letter in question.
Le petit chaperon rouge	Identifies foreign language words.
Warning!	Reserved for special warnings in order to emphasize the importance of words. Read out loud.

Note: Highlights a note. Generally, it gives additional information about a specific area.

Tip: Represents a tip. It could be general advice on how to perform a particular action, or hints about nice features, such as shortcuts, which could make your life easier.

Warning

Be very careful when you see this icon. It always means that very important information about a specific subject will be dealt with.

3.2. General Conventions

3.2.1. Commands Synopsis

The example below shows the symbols you will see when the writer describes the arguments of a command:

```
command <non literal argument> [--option={arg1,arg2,arg3}] [optional arg ...]
```

These conventions are standard and you will find them elsewhere such as in the `man` pages.

The "<" (lesser than) and ">" (greater than) symbols denote a **mandatory** argument not to be copied as is, which should be replaced according to your needs. For example, `<filename>` refers to the actual name of a file. If this name is `foo.txt` you should type `foo.txt`, not `<foo.txt>` or `<filename>`.

The square brackets ("[ ]") denote optional arguments, which you may or may not include in the command.

The ellipsis ("...") means an arbitrary number of arguments may be included.

The curly brackets ("{ }") contain the arguments authorized at this specific place. One of them is to be placed here.

3.2.2. Special Notations

From time to time, you will be asked to press, for example, the keys **Ctrl-R**, which means you need to press and hold the **Ctrl** key and tap the **R** character right after as well. The same applies for the **Alt** and **Shift** keys.

Note: We use capital letters to represent the letter keys; this doesn't mean that you have to type them capitalized. However, there might be programs where typing **R** is not the same than typing **r**. You will be informed when dealing with such programs.

Regarding menus, going to menu item File→Reload user config (**Ctrl-R**) means: click on the File text displayed on the menu (generally located in the upper-left of the window). Then in the pull-down menu, click on the Re-

load user config item. Furthermore you are informed that you can use the **Ctrl-R** key combination (as described above) to get the same result.

3.2.3. System-Generic Users

Whenever possible, we use two generic users in our examples:

Queen Pingusa	queen	This is our default user, used through most examples in this book.
Peter Pingus	peter	This user can be created afterward by the system administrator and is sometimes used to vary the text.

4. The Drakbug Reporting Tool

If you encounter unexpected behavior in Mandriva Linux-specific tools, Drakbug allows you to report it to the development team.

> **Note:** To be able to report bugs using Drakbug, you need a working Internet connection as well as an Drakbug account (`http://qa.mandriva.com/createaccount.cgi`).

To run Drakbug, go to the Help→Report Bug menu entry of the faulty tool, or run it from Mandriva Linux Control Center's own menu. Drakbug can also be triggered automatically by a crashed Mandriva Linux tool.

Figure 2. Reporting a Bug

1. Identify the Faulty Package

   In order to correctly report a bug, it is important to identify the package it is related to. To make this task easier, enter the application name in the Application Name (or Full Path) field and click on the Find Package button.

2. Fill in the Report

   Click on the Report button. Your web browser will then open. If you are not logged in to the Mandriva Bugzilla web site (`http://qa.mandriva.com/`) you will be asked to log in (or create an account if you do not have one). Once you are logged on the site, complete the bug report as completely and accurately as possible and click on Commit.

Chapter 1. Package Management

To begin with, a bit of vocabulary.

Package

    Software needs to be broken down into different files to ease its development and management. An application ends up being lots of pieces: the binaries, the documentation, the resources the application needs (images, icons, translations, sounds, etc.). A package is the set of all of an application's components, stored in a single file in a way that's very simple to install, update and remove.

Dependency

    Applications rely on software libraries or components made by different developers to perform a given set of functions, not part of the main functionality but needed to achieve it. A dependency is a package another package needs in order to work properly. Mandriva Linux's package management tool takes care of all the dependencies automatically.

Update

    Software is a living thing: new features are added, existing ones are enhanced and problems (bugs) are fixed. An update is a package which brings in some or all of these enhancements and fixes into an existing application. It is recommended that you check for updates often in order to keep your system in good shape and free from bugs and security threats.

Source

    A source is a repository of packages, and the place where packages are installed from. Sources for the media used during system installation are automatically created, you can add your own sources for updates and packages you find on the Internet.

Mandriva Linux uses the RPM packaging system. Mandriva Linux provides convenient tools to simplify package maintenance. The urpmi set of tools is command line based; here we will concentrate on Rpmdrake: Mandriva Linux's graphical software installation tool and the Software Media Manager. figure 1-1 shows the Software Management section of Mandriva Linux Control Center.

Figure 1-1. Software Management in the Mandriva Linux Control Center

Rpmdrake can be used in one of three modes: install

, remove

and update

, each explained in *Adding, Removing and Updating Software*, page 10. Media management is covered in *The Software Media Manager*, page 12.

1.1. Adding, Removing and Updating Software

When launching Rpmdrake you have to wait a few seconds while the package databases are scanned. Then you are presented with Rpmdrake's main interface.
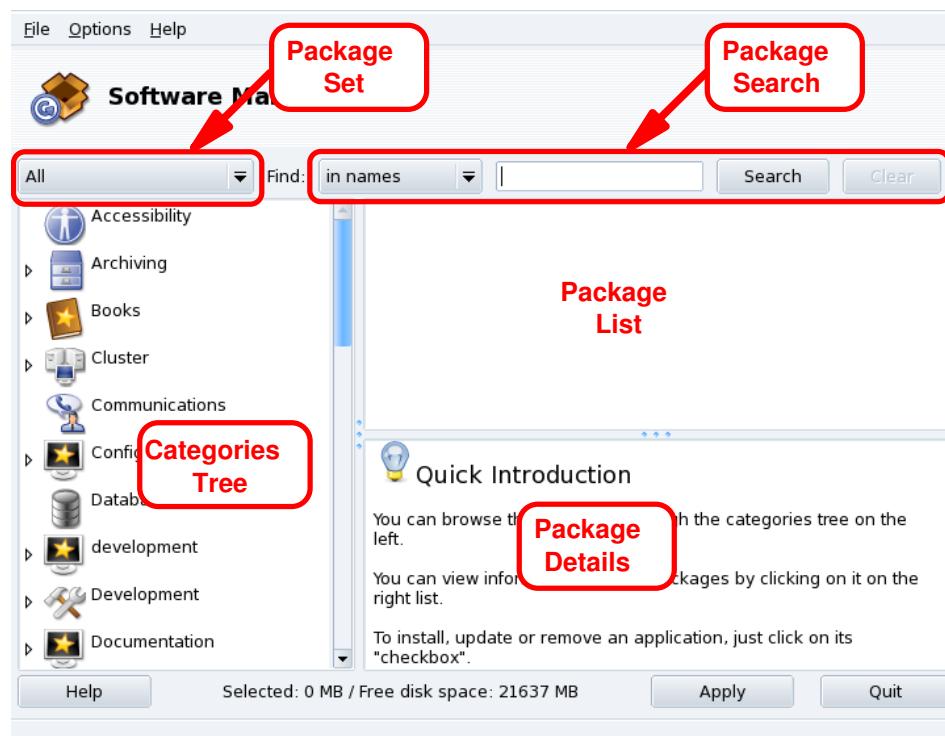
Figure 1-2. Rpmdrake Interface

Package Set. Use this pulldown list to select the types of package to be displayed: all of them (installed or not); only installed ones (to be uninstalled); only uninstalled ones (to be installed); and a few options for updated packages (all, security fixes, bug fixes, normal updates). Each time a package set is selected, the Categories Tree is rebuilt to display matching packages only.

Package Search. If you are not sure about a package name, use this facility to search for it. Type the string to be searched for, select the critera using the pulldown list, and click Search. You can search for package names (in names), package descriptions (in descriptions) and the package providing a given file (in file names).

> **Note:** If your software media repositories are configured to use the synthesized package lists (the summary synthesis files, not the full hdlist ones) you will not be able to look for the package providing a given file. You will only be able to search for package names and descriptions.

Categories Tree. To ease management, packages are classified into categories (Networking, Office, Games, Development, Graphics, etc.). Open a category to display packages which match the current criteria set using Package Set and Package Search.

Package List. Where currently matching packages (Set, Category and Search Criteria) are displayed. This is where you select packages to be installed, removed and upgraded.

Package Details. Displays details about the currently selected package in the Package List.

> **Note:** Additionally, a status bar in the lower part of the window displays messages about actions currently in progress or completed.

Actions on Packages

1. Limit List of Packages Displayed

   Use the Package Set pulldown list, the Categories Tree and, optionally, the Package Search facility to browse for packages to be installed, removed or updated.

2. Select Packages

   In the Packages List, select packages to be installed, removed or updated. If the checkbox by the package name is empty, it means that the package can be installed or upgraded, once selected it will be marked with the

   icon. If the checkbox by the package name has the

   icon, it means the package is already installed, select it for removal.

3. Apply Changes

   Once you are satisfied with your choices, click on Apply to perform the actual install, remove and upgrade of these packages. A new window appears, where you can see the progress of actions being taken. If you prefer to leave without doing anything, you can just click on Quit.

Handling Dependencies

It may happen that you select a package which requires dependencies (additional libraries or another tool) or which is a dependency of other packages. In this case Rpmdrake displays an information window allowing you to choose whether to accept the selected dependencies, to Cancel the operation, or to get More info on the operation (figure 1-3).

Figure 1-3. Dependency Alert Box

Alternative Dependencies. You may also want to install a package which requires dependencies, and various packages are capable of providing that dependency. The list of alternatives is then presented (figure 1-4). You may read the additional information presented by clicking the Info… button to help you choose the best alternative.

Figure 1-4. Alternative Packages

> **Note:** Due to dependencies, the disk space required by the selected packages might be greater than the size required by the chosen package by itself.

1.2. The Software Media Manager

Use this tool to configure the package media repositories. figure 1-5 shows some media already defined: "Main", "Contrib", etc. You can also add other software media: a CD from a magazine containing RPMs, a Web repository, etc.
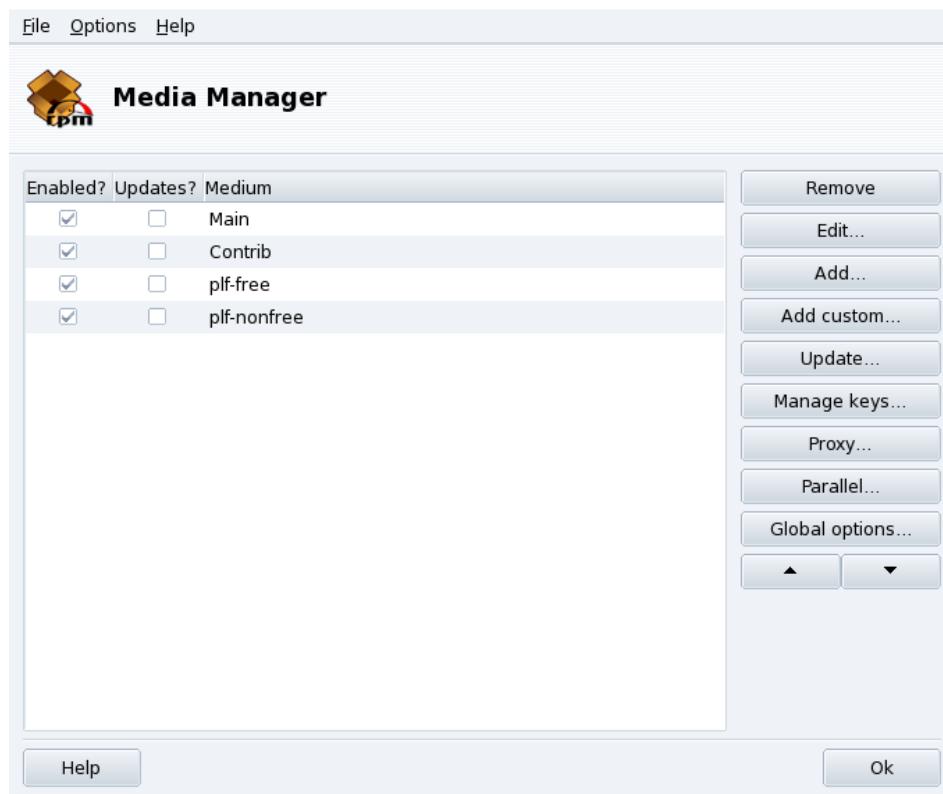
Figure 1-5. The "Software Media Manager"

Use check boxes of the left-hand columns to flag the repositories

Enabled?

Uncheck this box to temporarily disable the corresponding medium. The packages contained in this medium will not be available until you enable the medium again.

Updates?

> This box must be checked for update media, that is, media that contains updates of packages that are already in another medium, albeit with an older version number. Thus only update media are taken into account when looking for updates.

Action Buttons on the Right

Remove

> Discard a medium which you no longer use. Simply select the medium to be removed in the list and click this button.

Edit

> Change the medium's parameters: the URL or the relative path to the `synthesis/hdlist` (if you do not know what we are talking about it is wise to leave this window via Cancel instead of Save changes).

> In case you need to pass through a specific proxy to access this particular medium, you can configure it here by clicking on Proxy.

Add

> Add to your system all publicly available official package sources from Internet repositories. This is useful for example if you have a fast Internet connection or only have the first installation CD at hand. Choose a mirror geographically near to your location.

> After choosing a mirror and clicking Ok, package information for the source you chose is downloaded and all included packages will be available.

Add custom

> This button provides access to a new dialog, in which you define all needed parameters for a new software package medium. Please bear in mind that the required parameters, and available options, depend on the type of medium being defined.
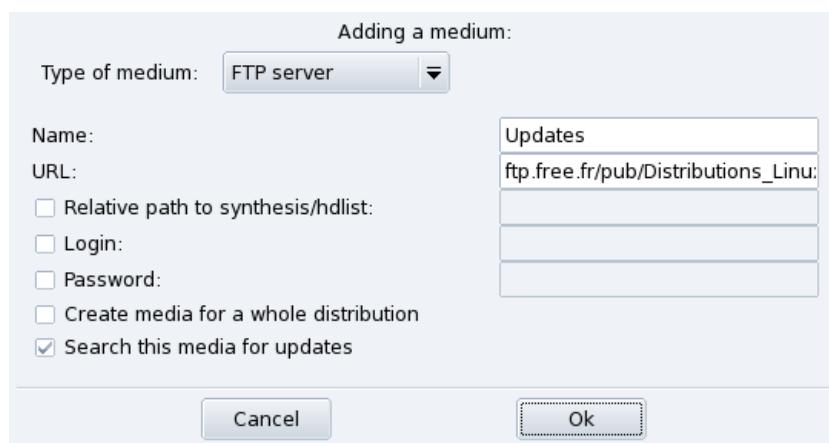
Figure 1-6. Adding a Custom Package Repository Media

Update

> You are shown a list of already defined, enabled, media; select the ones you want to update the list of available packages for, and click Update. This is useful for remote media to which new packages are being added.

Manage keys

> It is important that any package you install is authenticated. To do so, each package can be electronically signed with a "key", and you can allow/disallow keys on a per-medium basis. On figure 1-7, you can see that the Mandriva Linux key is allowed for medium "Main". Click on Add a key to allow another key for the selected medium (beware, do this with care, as with all security-related questions), and on Remove key to remove a key from the selected medium.

Figure 1-7. Package Repository Authentication Key Management

Proxy

> If you are sitting behind a firewall and you still need to access remote media (especially for package updates), you can do so if you have a proxy server which leads to the Internet (at least in an area where you can find a package server). Normally it should be enough to fill in the Proxy hostname to get it working (figure 1-8). If you need a user / password combination to get through the proxy, you can also specify these here. Just confirm your changes by clicking on OK and you are done.

Figure 1-8. Specifying a Proxy for Remote Media

Parallel

> If you are running a large network of computers, you may want to install a package on all the computers in parallel; this button opens a dialog window allowing the configuration of the "Parallel" mode. As it is rather complicated and only useful to a limited group of people, this short introduction will not give further details about it.

Global options

> This button allows you to configure the program used to retrieve remote packages and whether the packages should be checked against a key. These choices affect all package sources.

Up and Down arrows

> These buttons allow changing the order in which sources will be used when installing packages. By default, the newest version of a given package will always be installed, but if the same version is found on two different media, the one from the first medium in the list will be installed.

> > **Tip:** Therefore, it is better to move fastest media up...

Chapter 2. Controlling a Remote Machine

Being able to remotely control another machine offers many possibilities, from remote technical assistance to teaching how an application works. In this chapter we describe the configuration and usage of Rfbdrake, a tool to easily set up a virtual network computing environment under Mandriva Linux.

2.1. Concepts

Here are a few concepts:

Virtual Network Computing (VNC)

An environment which allows you to interact with a remote computer "as if you were sitting in front of that computer". The computers don't have to be of the same type, nor do they have to be running the same OS: they only need a working TCP/IP network connection.

Controlled Computer

This is the computer to be controlled without the need, or the possibility, to be actually sitting at its console. It is remote from your location. Also called the "server".

Controlling Computer

This is the computer in front of which you're sitting, from where you interact with the controlled (remote) computer. Also called the "viewer".

2.2. Installation and Setup

Make sure the `rfbdrake` package is installed and then access Rfbdrake through the Mandriva Linux Control Center: an Online Administration section is accessible from which you can start the Remote Control of another machine (Linux/Unix, Windows) utility.

2.2.1. Controlled Computer Setup

Two scenarios can occur here: either you, or the person you are assisting, can access Rfbdrake (local access); or not (typically remote administration tasks), then you need to follow the remote access procedure, described in *Remote Administration Access*, page 16.

> **Firewall:** If the system to be controlled is behind a firewall, then you have to make sure that port `tcp/5900+N` is opened on the firewall, where `N` is the VNC server display number.

2.2.1.1. Local Access

For the machine that will act as the controlled (server) computer, select the Allow control of my machine (linux server) option. Fill the Set Password field. This is mandatory or Rfbdrake will complain. Please bear in mind that this password is not related to the user's local/remote account password in any way.
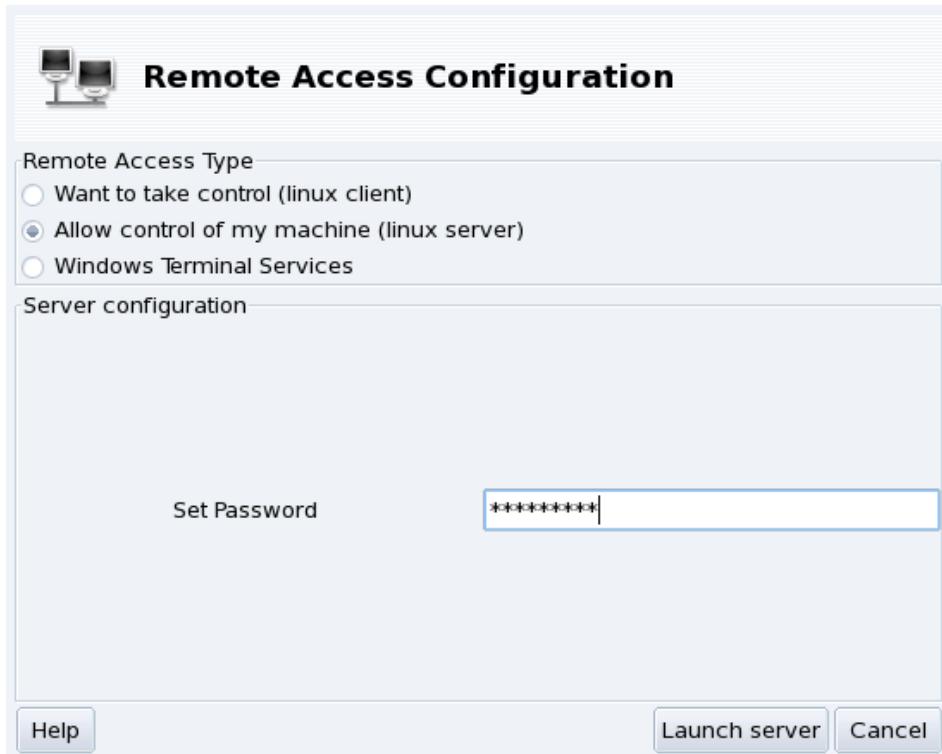
Figure 2-1. Server Options

 Once you click on Launch server this icon indicates that the computer is ready to accept incoming VNC connections. Closing it will stop the VNC server. Right-click on it to access a pop-up menu with some options.

2.2.1.2. Remote Administration Access

1. Make sure the `tightvnc-server` package is installed on the remote machine.

2. Connect to the remote machine using `ssh`, and become root on it.

3. If it's not already running, start the VNC server by executing `vncserver` in a console. If this is the first time `vncserver` is run on the system with that user account, then you have to enter the password clients will have to use to connect and confirm it. The system informs you which display number clients have to use. Run `vncserver -kill :DISPLAY_NUMBER` when you no longer need the VNC server.

Then connect as a client to control the remote machine (see *Controlling Computer Setup*, page 16).

2.2.2. Controlling Computer Setup
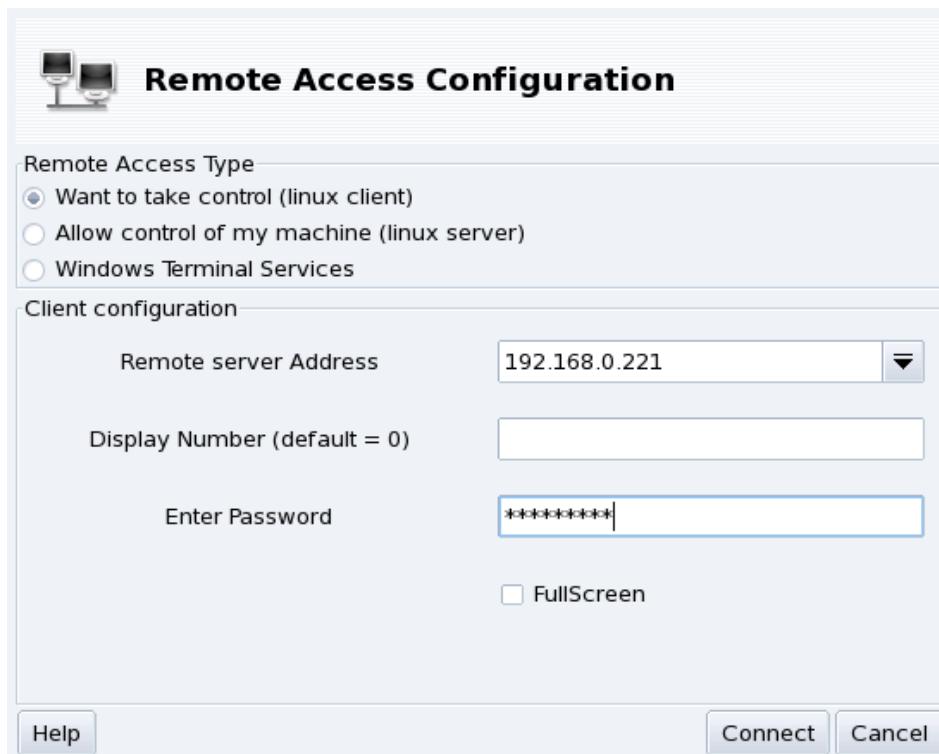
Figure 2-2. Viewer Options

1. On the machine which will act as the controller (viewer) computer, run Rfbdrake and select the Want to take control (linux client) option.

2. Fill the Remote server Address pull-down list with the IP address or hostname of the computer to be controlled.

3. Fill the Display Number field with the remote computer's display number, or leave it empty to use the default (display number 0).

4. Enter the server password in the Enter Password field.

5. Optionally, put a mark in the FullScreen check-box to have the remote computer's desktop use all of the controller computer's screen. Otherwise the remote desktop will be displayed in a window.

6. Once you are satisfied with your settings, click on the Connect button to access the remote computer.

2.3. Connecting to a Windows® Terminal Server
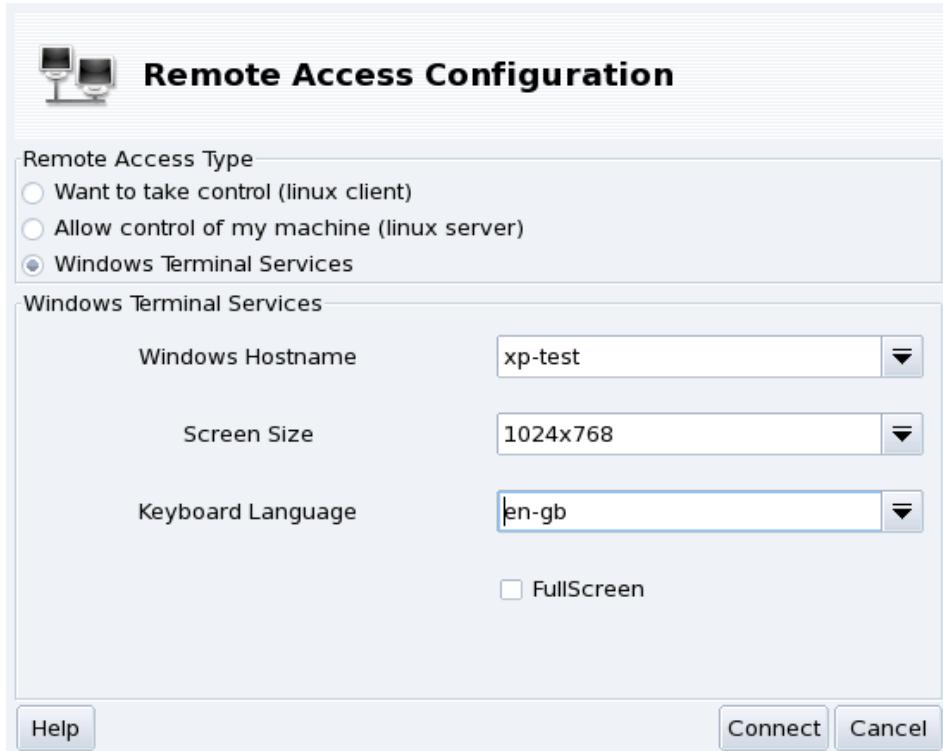
Figure 2-3. Windows Terminal Services Options

1. Select the Windows Terminal Services option to connect to Terminal Services on a Windows® machine.

2. Fill the Windows Hostname pull-down list with the hostname of the Windows® machine or its IP address.

3. Select a desktop size in the Screen Size pull-down list and a language for the keyboard in the Keyboard Language pull-down list.

4. Finally, click on the Connect button once you're satisfied with your settings.

2.4. Remote Control in Action

Once you connect to the remote computer you see its desktop and you are able to perform **any** action as if you were sitting in front of it.
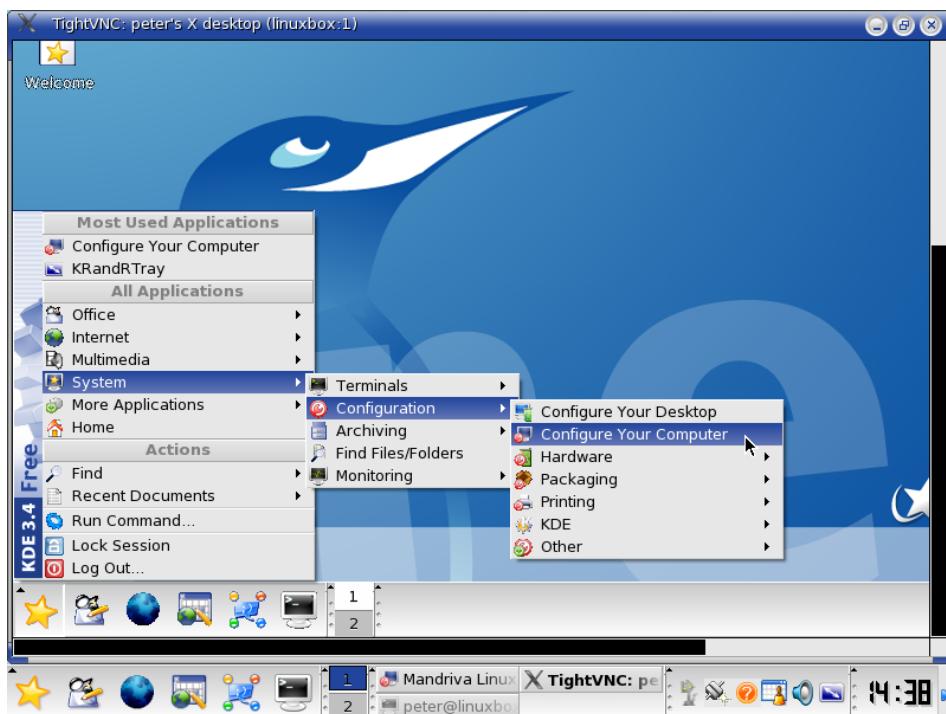
Figure 2-4. Controlling a Remote Computer

> **The Mouse Cursor:** The mouse cursor becomes a round point and the remote computer's arrow-cursor will "follow" it. This can prove useful to keep track of where the cursor is at any given time.

Link Speed and Responsiveness. The limiting factor of the response time of the remote computer is the speed of the link to it. For LAN connections (typically 100 Mbps), you will feel that you're really in front of the remote computer. For Internet connections (typically between 56 Kbps and 1-2 Mbps), don't expect "instantaneous" response from the controlled computer.

Disconnection. Once you've finished using the remote computer, you can disconnect from it by closing the VNC viewer window. If you're using the full-screen mode, press the **F8** key and select the Quit viewer option from the menu which pops up.

2.5. More Documentation

This short introduction to VNC has hopefully shown you some of the possibilities of remotely controlling computers. The options are endless, please refer to the TightVNC Documentation (`http://www.tightvnc.com/docs.html`) and to the VNC Documentation (`http://www.realvnc.com/documentation.html`) web sites.

Chapter 3. "Hardware" Section

3.1. Configuring your Hardware

3.1.1. Hardware Detection and Configuration

The HardDrake project has been developed to simplify hardware detection and configuration under GNU/Linux by providing a user-friendly interface.

3.1.1.1. What Is HardDrake?

HardDrake is a service for hardware detection, run at system boot time, and also a full GUI-based tool which ties together many of the tools already included in a GNU/Linux distribution. It automates and simplifies the process of installing new hardware. For the most part, HardDrake will be able to detect most devices.

On one hand, HardDrake is used to display information, and on the other, it can launch configuration tools. With its easy-to-use interface, you can browse all the hardware your system contains.

HardDrake uses the "ldetect" engine, so if your new hardware is not detected, you may try to upgrade the `ldetect` library itself and its hardware database, located in the `ldetect-lst` package.

3.1.1.2. Usage

To launch HardDrake, you can start it through:

- the Mandriva Linux Control Center: click on the Hardware category, and then on the Hardware icon.
- a terminal: type `harddrake2` as `root`. You can also pass parameters to HardDrake through the command line (type `harddrake2 -h` to get a list of possible parameters).
- the desktop: go to the main menu. The HardDrake entry is in the System+Configuration+Hardware→HardDrake sub-menu.

After all devices have been detected, the main HardDrake window appears (see figure 3-1).

On the left, you can see the device tree showing you all of the hardware categories.
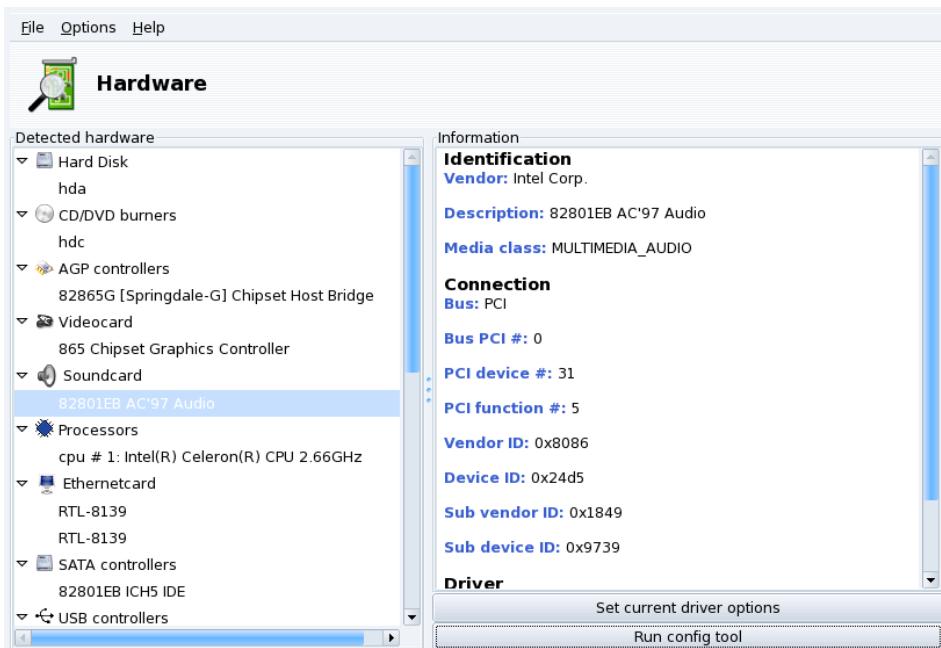
Figure 3-1. Selected Device

By selecting a device, you will see additional information about it in the right frame. To better understand the meaning of the information presented, you can consult the help page accessible by choosing Help→Fields description from the menu.

Depending on the device selected, two other buttons may appear:

- **Set current driver options.** This pops up a window with all the module device parameters listed. **For experts only!**

- **Run config tool.** Launches the Mandriva Linux configuration tool (available through the Mandriva Linux Control Center) associated with that device.

Unknown hardware. A special category called `Unknown/Others` might also show up, containing all the currently unknown hardware in your system, as well as known hardware that does not fit into the existing categories (such as thermal sensors, random number generators, etc.).

Auto-detection of special devices. You can also toggle the entries in the Options menu to enable automatic detection of some hardware which wouldn't have been detected otherwise. You need to restart HardDrake for those changes to have effect.

3.1.2. Problems/Troubleshooting

If you think you have found a bug related to HardDrake, report it using the Mandriva Linux bug reporting tool.

Sound Cards. HardDrake does not probe for ISA PnP devices. If you have an ISA PnP sound card, run `sndconfig` or `alsaconf` from the command line. You may need to install the `sndconfig` package or the `alsa-utils` package.

3.2. Controlling the Graphical Configuration

This set of tools allows you to configure your graphical display. With it you will be able to change your video card, your resolution and your monitor. It can be useful if you happen to change one of your graphical components after the initial installation.

> **If you Don't See Graphical Login at Boot:** If the graphical server cannot start because of a configuration error, a dialog offers to reconfigure the graphical server. You will get a tool similar to the one described in *Controlling All Video Parameters*, page 24, but in text mode.

The graphical configuration tools are accessible through different icons in the Mandriva Linux Control Center Hardware section.

3.2.1. Changing the Monitor

This tool allows you to change the monitor type currently in use. When you click on it a window pops up, listing many monitor models (see figure 3-2). If your monitor was automatically detected it is listed as Plug'n Play along with its model.
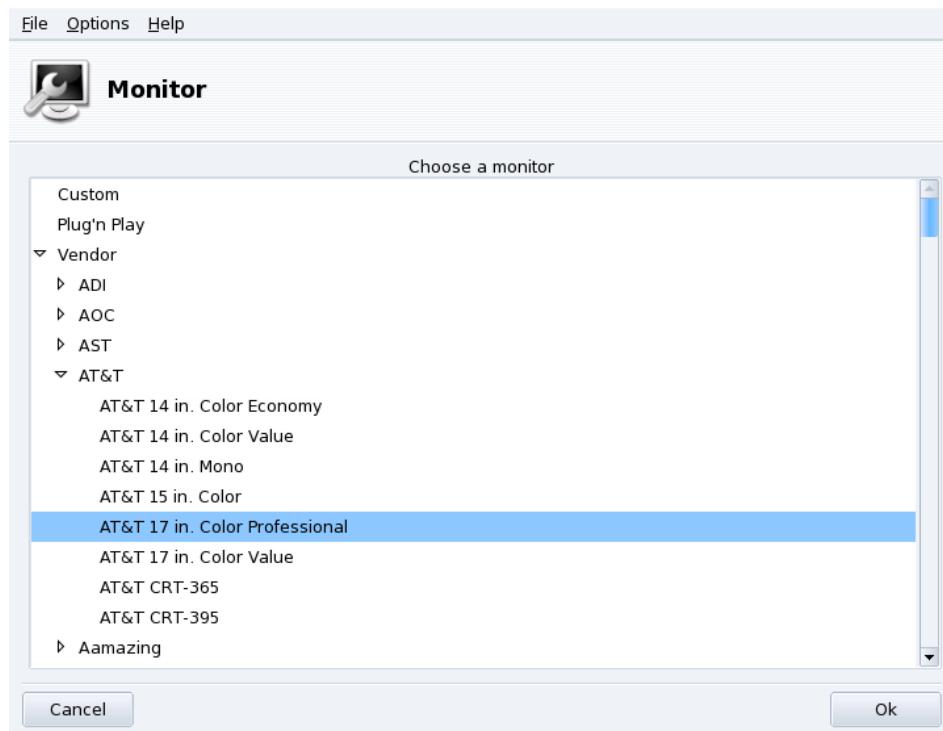
Figure 3-2. Choosing a New Monitor

If your monitor wasn't automatically detected, you can choose it from the list. If you don't find your monitor or a compatible one, choose one with parameters corresponding to your own monitor from the Generic entry, at the bottom.

3.2.2. Changing Resolution

This tool enables you to change the current screen resolution (`800x600`, `1024x768`, etc.) and the color depth. Simply choose the one you wish to use.
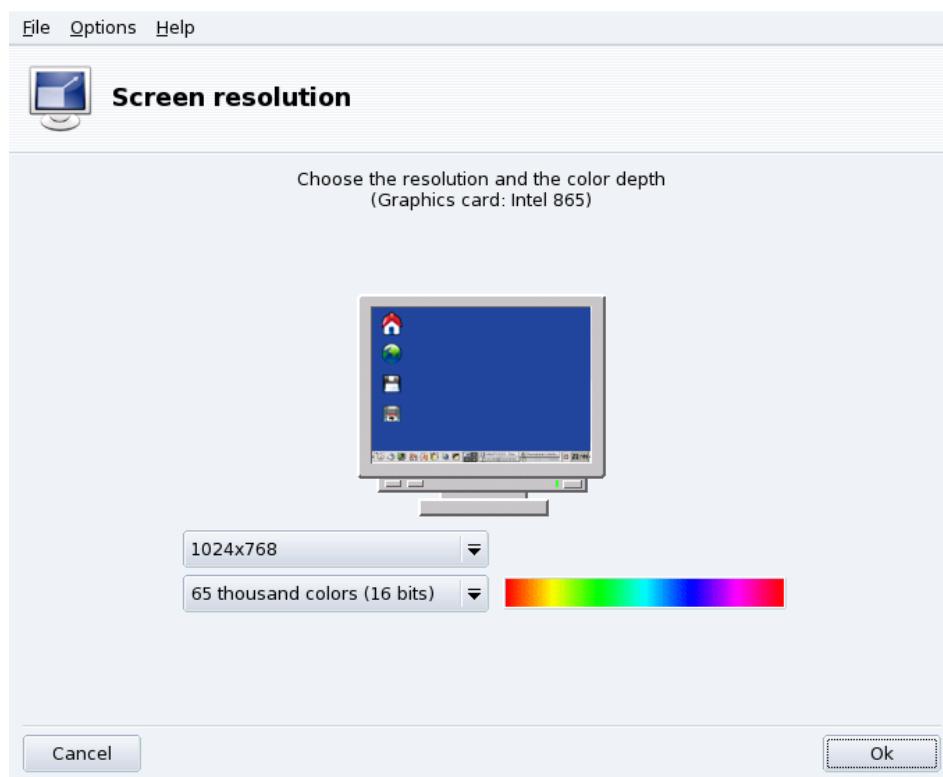
Figure 3-3. Changing the Resolution of your Screen

The monitor in the window displays what the desktop will look like with the chosen configuration (see figure 3-3). If it looks good, click on OK. The changes will be activated after you quit and restart your graphical environment.

Monitor and Resolution Ratio. By default, the available resolution list only shows resolutions supported by your video card and monitor combination. There is a special entry named Other which adds more possible resolutions along with their ratios. Bear in mind that most monitors are designed with a `4:3` horizontal vs. vertical ratio.

3.2.3. Controlling All Video Parameters

If you happen to change your video card after installing your system, or want to have full control over the graphic configuration, run this tool.

Figure 3-4. XFdrake Main Window

The first three buttons allow you to change certain aspects of the graphical configuration:

Graphic Card

> The button displays the name of the graphic card currently configured. If you wish to change it, just click on it. Depending on your card, different servers may be available, with or without 3D acceleration. You may need to try different ones until you get the best result.
>
> In case you cannot find the graphic card you have, but you know which driver supports it, select it from the Xorg entry at the bottom.

Monitor

> Enables you to change the monitor with the tool described in *Changing the Monitor*, page 23.

Resolution

> Enables you to change the pixel resolution and the color depth with the tool described in *Changing Resolution*, page 23.

> **Changing the Resolution Using the Desktop Applet:** If you are using KDE you can also change the screen resolution on the fly by using the screen resize applet, accessible choosing System+Configuration+Hardware→KRandRTray from the main menu.

Then, there are more buttons:

Test

> Click on this button to verify that your modifications actually work. It is highly recommended that you do test it, because if it does not work, it will be harder to recover a working graphical environment later. If the test fails simply wait until it ends. If you are not satisfied with the suggested settings, choose No during the test, and you will be returned to XFdrake's main menu.

> **If the Test is Not Available:** Depending on your video card, video testing may not be available. You will be warned of such a situation. If it happens that the settings are incorrect and your display does not work, launch `XFdrake` as `root` in the console to use XFdrake's text version.

Options

Graphic card options

Depending on your hardware capabilities, you can choose here to activate or disable specific features such as 3D acceleration or special visual effects (translucency).

Graphical interface at startup

This option allows you to choose whether you want your machine to automatically switch to a graphical interface at boot. Obviously, you may want to select the No option if your machine is to act as a server, or if you were not successful in getting the display configured.

Quit

If you modified your graphical display in some way, the current configuration will be displayed and XFdrake will ask you whether you want to keep your changes or not. This is your last chance to go back to the old configuration. If all seems OK, click on Yes. If you wish to restore the previous parameters, click on No.

The changes will be activated after you confirm them and restart your graphical environment.

3.3. Configuring the 3D Desktop

This tool, accessible from the Hardware section of Mandriva Linux Control Center, lets you configure the "3D desktop" for stunning visual effects on your desktop, together with a change from a flat desktop to a cubic one.
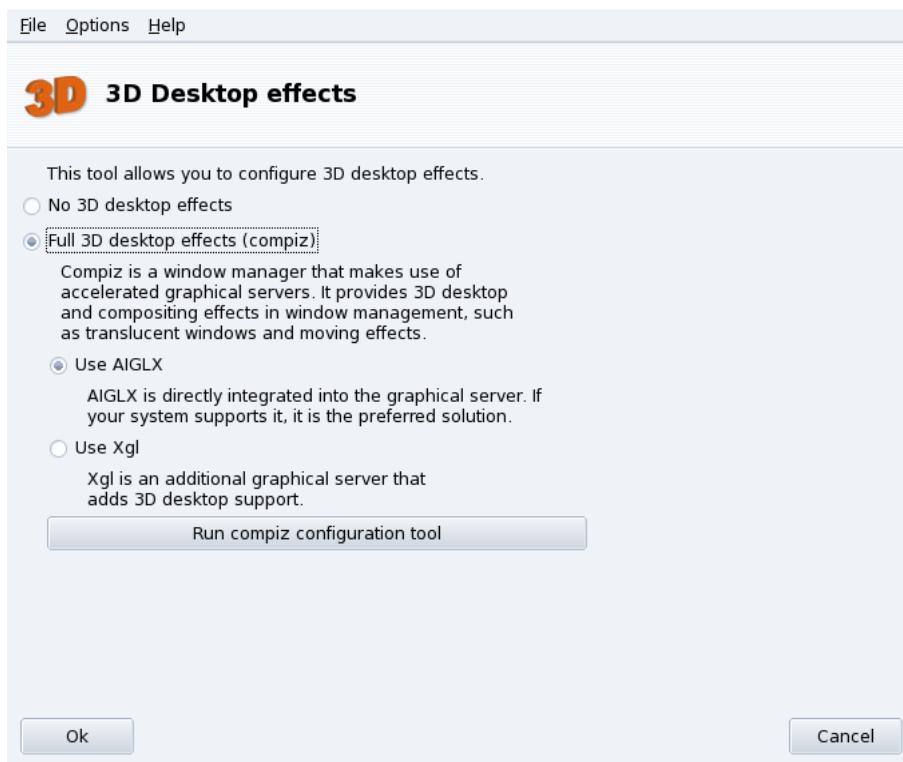

Figure 3-5. Activating 3D Desktop Effects

Activate the 3D Desktop

1. The first time you run Drak3D a few required packages may be installed; then you are presented with its main window (see figure 3-5).

2. Select the Full 3D desktop effects (compiz) option to enable the 3D desktop. There are two approaches: AIGLX and Xgl, Drak3D selects the most appropriate one for you according to your hardware.

3. Click Run compiz configuration tool to fully customize every single aspect of the 3D desktop support, a new window appears for you to set all parameters to your liking.

> **About desktops:** Once the 3D desktop is active, the number of virtual desktops as shown by the desktop manager (KDE or GNOME) will be reduced to one. You now have instead viewports (the cube faces) for your virtual desktops, explore and enjoy them!

4. Once you are satisfied with your settings, apply them by clicking Ok; they take effect the next time you enter your graphical session.

Disable 3D. Select the No 3D desktop effects option to disable the 3D desktop completely, and return to your "flat" desktop.

3.4. Setting up a TV Card with DrakxTV

This tool will configure your TV tuner card so you can watch television on your computer display.

Check your Hardware Compatibility. First of all you should make sure your card is supported by Mandriva Linux by consulting the Hardware Compatibility page (`http://www.mandriva.com/hardware`) or the BTTV driver home page (`http://linux.bytesex.org/v4l2/bttv.html/`).

> **Do I Need This Tool?:** Modern TV viewing programs (such as kdetv or TVtime) have their own configuration and channel-scanning interface embedded. You only need to run DrakxTV if you plan to use xawtv with old TV cards based on the btxxx or saa71xx chips.

> **Tip:** Make sure your card is correctly connected to your antenna or cable, so that channel scanning runs properly.
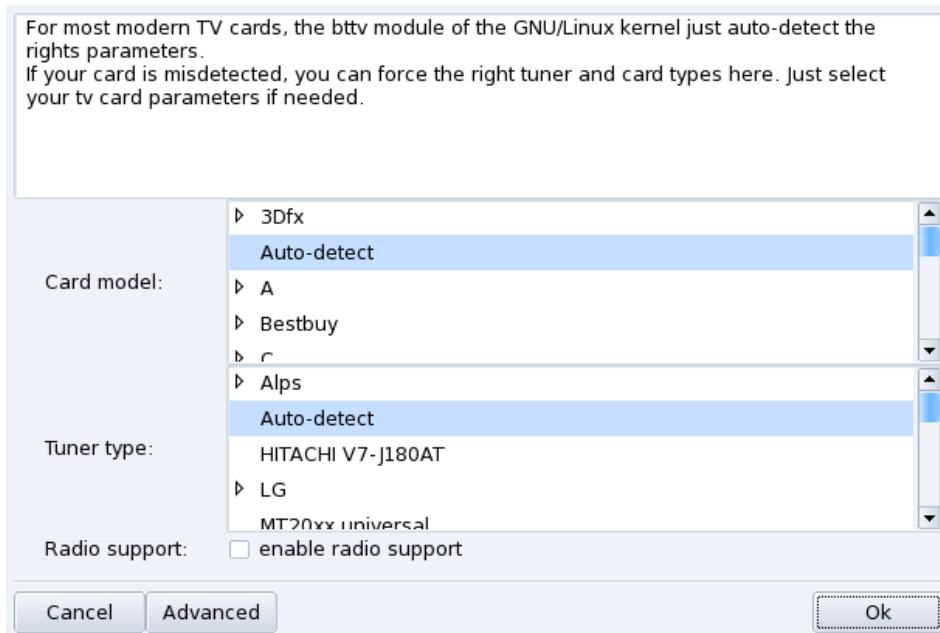
Figure 3-6. Choosing the TV Card Model

When you first launch the tool, and if a TV card is detected, the main configuration dialog (figure 3-6) will appear. Leave the default Auto-detect entries and press OK. If you notice afterward that your card was not properly configured, you can run DrakxTV again and select the proper card.
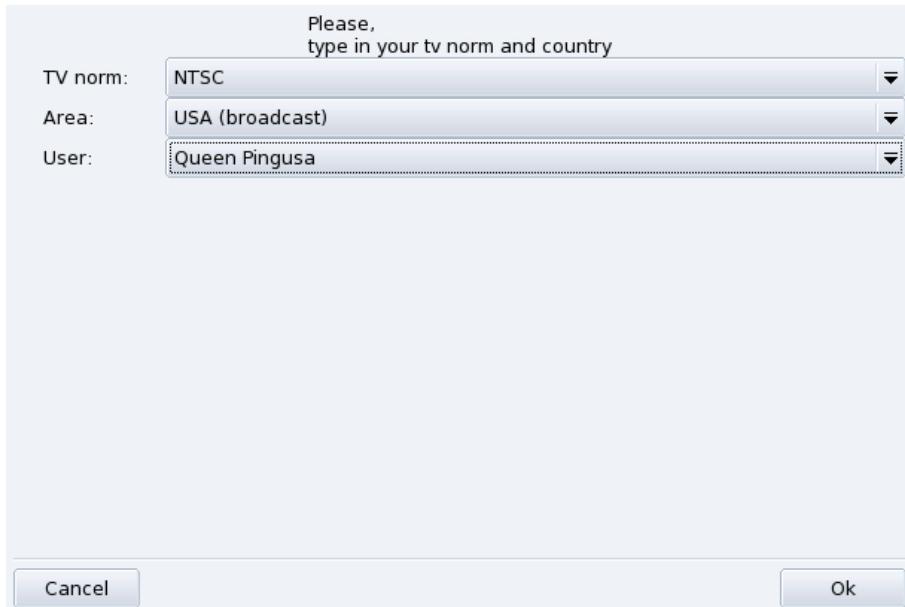
Figure 3-7. Choosing the TV Norm and Country

You simply need to inform DrakxTV about the norm used for the television signal you receive, and the country you're in. You also have to select the user who is going to use xawtv so that his configuration file is created.

After you press OK, DrakxTV will begin automatic channel scanning. Once this is done, your TV setup will be complete and you will be able to watch television on your computer using xawtv. Other applications allowing to you watch TV under Mandriva Linux are kdetv, tvtime and zapping.

3.5. Changing your Keyboard Layout

This tool allows you to define another keyboard layout, useful when the keyboard you want to use is different from the one chosen at installation time.
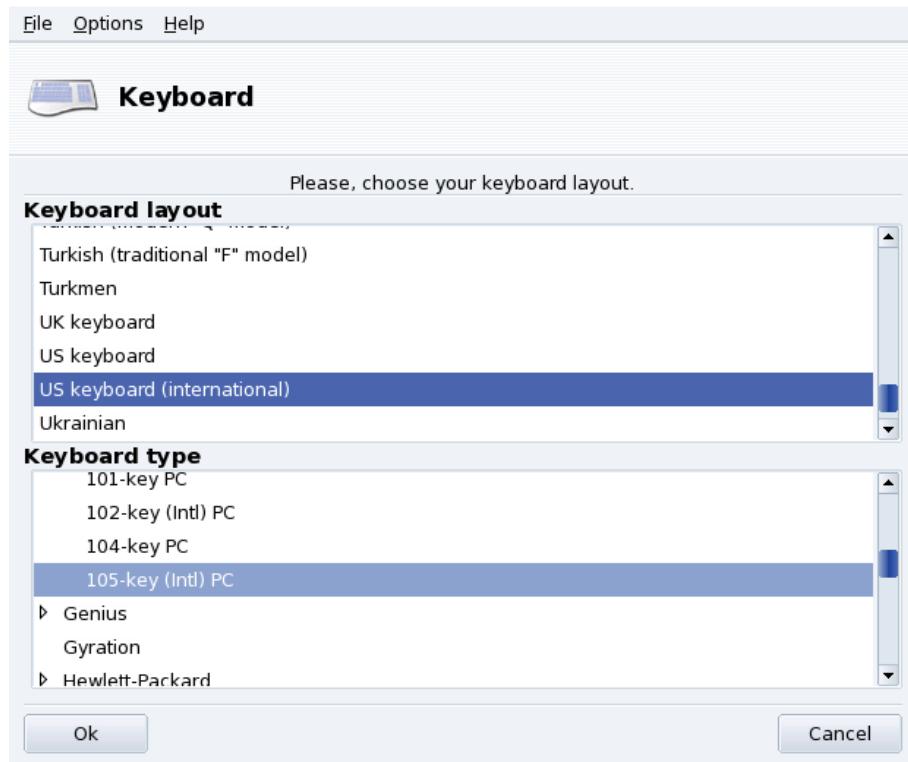
Figure 3-8. Choosing a Different Keyboard Layout

Select your keyboard's language and then its model from the lists shown in figure 3-8. If you own a multimedia keyboard and it is listed in the manufacturer list, chances are most multimedia keys on it will be supported. Otherwise, choose your keyboard type under the Generic branch. Changes are effective immediately after clicking OK.

> **Note:** If you choose a keyboard layout based on a non-Latin alphabet, the next dialog will ask you to choose the key combination that will switch the keyboard configuration between the Latin and non-Latin layouts.

3.6. Changing your Mouse

This tool enables you to set up a different mouse, which is useful if the mouse you are currently using is not the same as the one you chose at installation time.

> **Note:** Synaptics Touchpad function is automatically configured to work with almost every touch pad found on notebook computers. The same goes for Wacom® tablets.
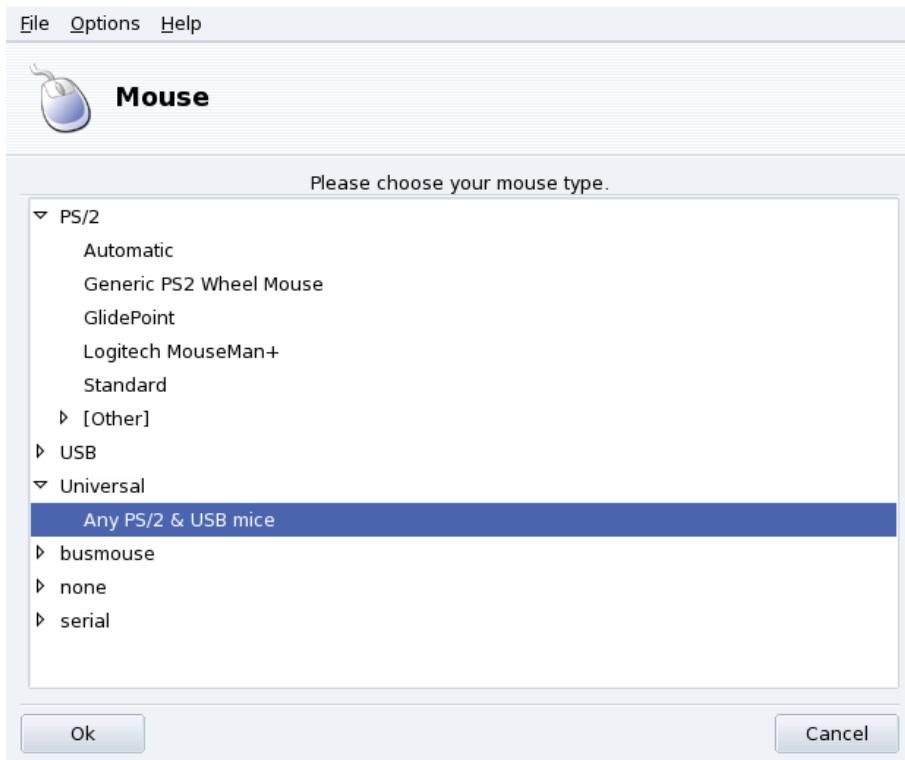
Figure 3-9. Choosing a Different Mouse

Mice are sorted into a tree according to their connection type and model (see figure 3-9). Highlight the mouse of your choice and click OK. Changes take effect immediately after the mouse test is done.

> **Tip:** The Any PS/2 & USB mice option works with virtually all modern mice.

3.7. Configuring Printers with PrinterDrake

 This tool allows you to:

- Configure a newly installed printer;
- configure your machine to act as a server for a printer connected to your local network;
- set up your machine to access network printers served by other servers.

3.7.1. Automatic Installation

If you connect and power on a USB printer, a dialog pops up.

Figure 3-10. A new Printer was Detected

Deactivate Automatic Detection. If you don't want the "automatic setup" popup to show again, check Do not setup printer automatically again.

Then just click Ok, all required packages will be installed, and the printer configured for you to let you use it right away: nothing else to do!

Configuration. It is however recommended that you check the printer default parameters, especially paper size. To do this launch PrinterDrake from the Mandriva Linux Control Center and follow the instructions from *Reconfiguring an Existing Printer*, page 37.

3.7.2. Manual Configuration

> **Tip:** If you have just installed a printer that wasn't available when you installed Mandriva Linux, make sure it is correctly connected and powered on before launching the configuration tool.

When you first launch the PrinterDrake tool, it may be in one of these states:

3.7.2.1. There is no printer directly connected to the computer.
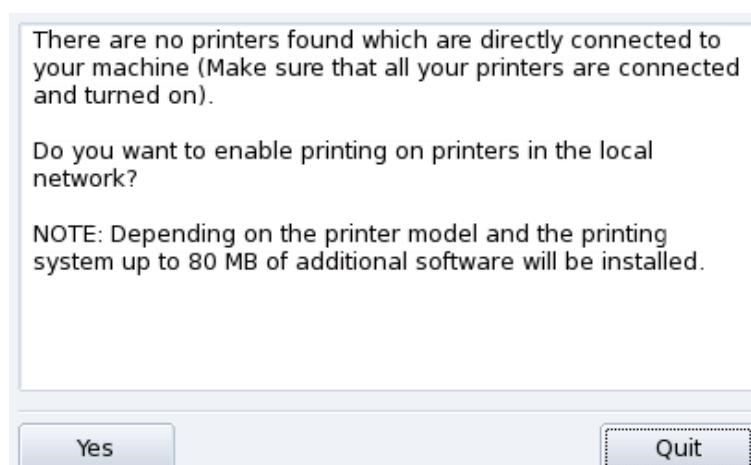
Figure 3-11. Activate Printing

The tool did not detect any local printers. However you can print on network printers, or manually installed printers which weren't detected by clicking on Yes.
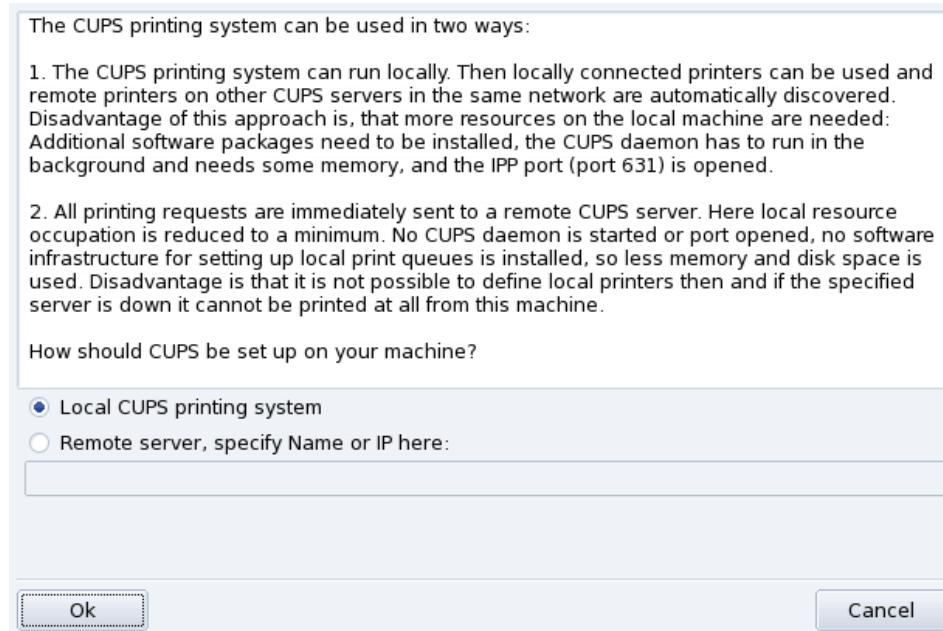
Figure 3-12. Activating Network Printers

- Select the Local CUPS printing system option if you wish to configure your machine to act as a print server for either a local printer which was not detected, or a networked printer connected to your local network.

  Any required software will be installed and then the main configuration interface (see figure 3-14) appears. Click on Add Printer to install the network printer.

- Select the Remote server option if you wish to be able to print on printers served by another CUPS print server on the network. Your applications will immediately have access to all public printers served by that server. You only need to provide the hostname or IP address of that server in the field (ask your system administrator).

  When this is done, the main configuration interface (see figure 3-14) appears. The Configured on other machines tab will be filled with the available network printers.

3.7.2.2. New Printer Detected

The following window appears when PrinterDrake detects a new printer at launch time.

The following printers

- HP DeskJet 990C
- HP OfficeJet 6100 Series

are directly connected to your system (Make sure that all your printers are connected and turned on).

Do you want to enable printing on the printers mentioned above or on printers in the local network?

NOTE: Depending on the printer model and the printing system up to 80 MB of additional software will be installed.

Yes   Quit

Figure 3-13. A New Printer Is Detected

Simply confirm the automatic installation of the new printer. The main configuration interface (see figure 3-14) is then displayed. Make sure you check that the printer parameters fit your needs (see *Reconfiguring an Existing Printer*, page 37).

3.7.2.3. A Printer is Already Configured

The main configuration interface (see figure 3-14) is shown. Make sure that the printer parameters fit your needs (see *Reconfiguring an Existing Printer*, page 37).

3.7.3. The Printer Management Interface

Local and Remote Printers. Use the printer configuration tool's first tab for locally connected printers (Configured on this machine), and the other tab for printers available on your local network (Configured on other machines).
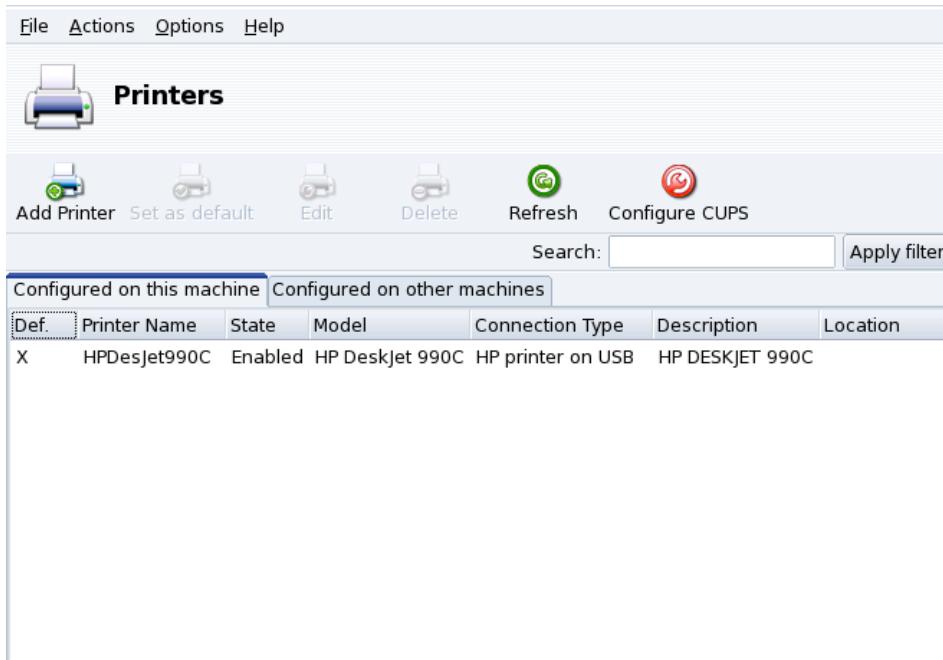
Figure 3-14. Managing Printers

The following buttons give you access to all available maintenance tasks:

- Add Printer: launches the printer configuration wizard described in *The Printer Configuration Wizard*, page 35.

- Set as default: sets the selected printer as the default printer when no specific printer is chosen at print time. A cross appears in the Def. column of that printer.

- Edit: opens the printer configuration dialog described in *Reconfiguring an Existing Printer*, page 37.

- Delete: removes the selected printer from the available printer pool.

- Refresh: updates the list of available printers, especially useful for networked printers.

- Configure CUPS: by default, your system is open. PrinterDrake uses all of the network's available printers and shares all of its local printers with the local network. Click on this button if you don't want to access network printers, or if you want to restrict the access to your local printers. This dialog also lets you configure access to print servers outside the local network (see *Print Server General Configuration*, page 33).

> **Note:** The Options→Expert mode menu adds extra features to the tool. See *Expert Mode*, page 38.

3.7.4. Print Server General Configuration

The Configure CUPS button allows you to control the behavior of printers connected to your machine and to your network.
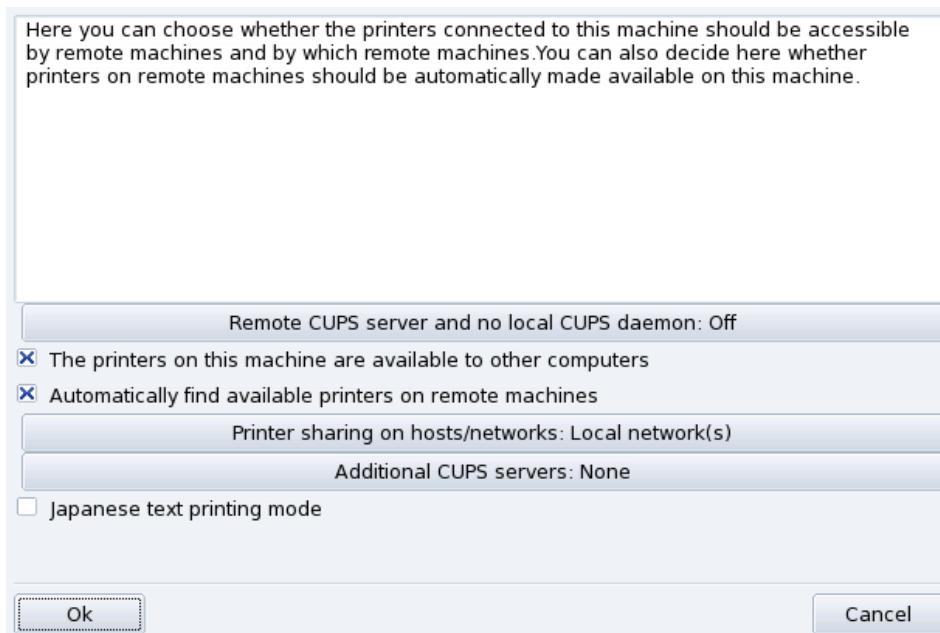
Figure 3-15. CUPS Printer Server Configuration

This dialog enables you to switch between the client and server printing modes through the Remote CUPS server and no local CUPS daemon button.

This button enables you to select between two remote server access methods.

In the first method your server **must** have a CUPS daemon running and be listening on port `631` in order to manage the print queue and to listen for jobs coming in from applications. In this case the CUPS server broadcasts its presence to the entire network. This is the default configuration.

In the second method, the CUPS daemon is still required to manage the queue and to handle jobs coming in on port `631`, but it does not broadcast its presence to the network. In this case the clients do not need to run a CUPS daemon, instead they have a configuration file which contains the IP address of the server. In this way the clients know they can sent jobs directly to the IP address.

	Advantages	Disadvantages
Method 1	No client configuration required	Runs with at least one open port and consumes extra machine resources
Method 2	No local printing system. No open ports	If the IP of the server changes or the client changes to another network, then reconfiguration is required.

Table 3-1. Considerations

3.7.4.1. Client Mode

In this mode the local CUPS daemon will be stopped and all printing requests go directly to the server specified below. Note that it is not possible to define local print queues then and if the specified server is down it cannot be printed at all from this machine.

○ Off
◉ On, Name or IP of remote server:
printserver.company.net

Ok   Cancel
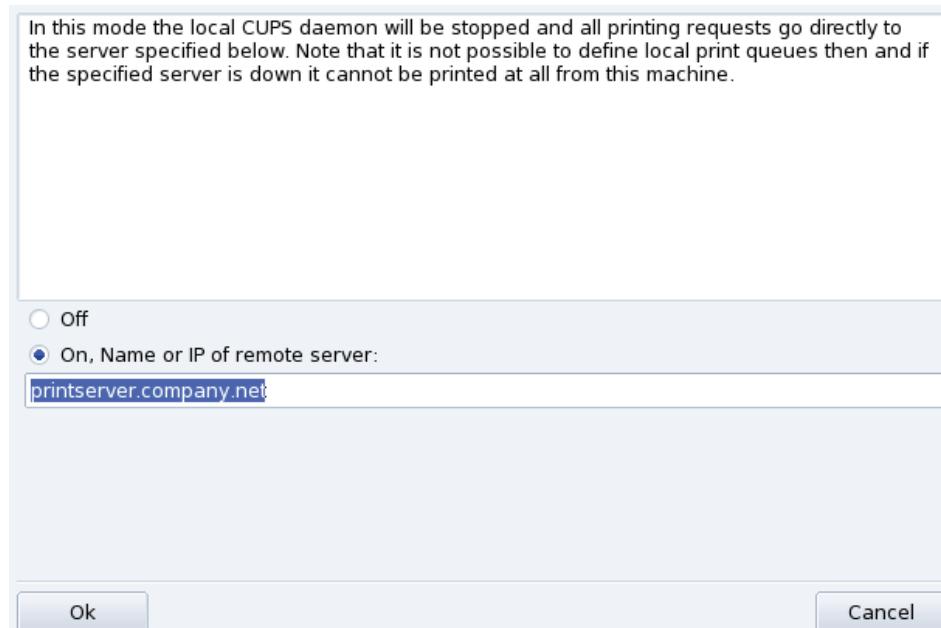
Figure 3-16. Client Mode Configuration

Select the On option to connect to another printer server. Then you only need to specify the name or IP address of that server in the next field below.

If you choose this mode, your printing configuration is now finished. Accept the options by clicking the OK buttons, and you will be able to check the list of available printers in the Configured on other machines tab of the main interface (see figure 3-14).

3.7.4.2. Server Mode

If you want your machine to access locally connected printers (through parallel or USB ports), or network printers not already configured on another server, you need to select the Off option. Click OK to fine tune your printer server (see figure 3-15).

A number of options are available to further secure and enhance your print server features:

The printers on this machine are available to other computers

> Allows other computers to print on printers configured locally. Remember to restrict access by clicking on Printer sharing on hosts/networks (see below).

Automatically find available printers on remote machines

> Tells your print server to automatically make all printers found on other servers available to the local network, as if they were locally connected to your print server. This way your system's users are able to print on any printer the print server can "see". If the remote printers you intend to use are served by a server not on your local network, you can still tell the print server to use them with the Additional CUPS servers button (see below).

Printer sharing on hosts/networks

> Allows you to specify from which networks the local printers are made available.

Additional CUPS servers

> Allows you to specify one or more CUPS servers to which you can connect and access printers. Specify the IP address and port of the CUPS server in the dialog.

Japanese text printing mode

> Replaces the original text filter for one more suited to Japanese texts, but with less features. Use it if you have to print Japanese text-only files.

3.7.5. The Printer Configuration Wizard

Click on Add printer and the configuration wizard comes up.

3.7.5.1. Detect Printers or Specify Access Path

The first step serves to either specify an access address to a network printer, or to activate auto-detection of locally connected printers, network printers, and finally printers served by SMB (Windows®) servers.
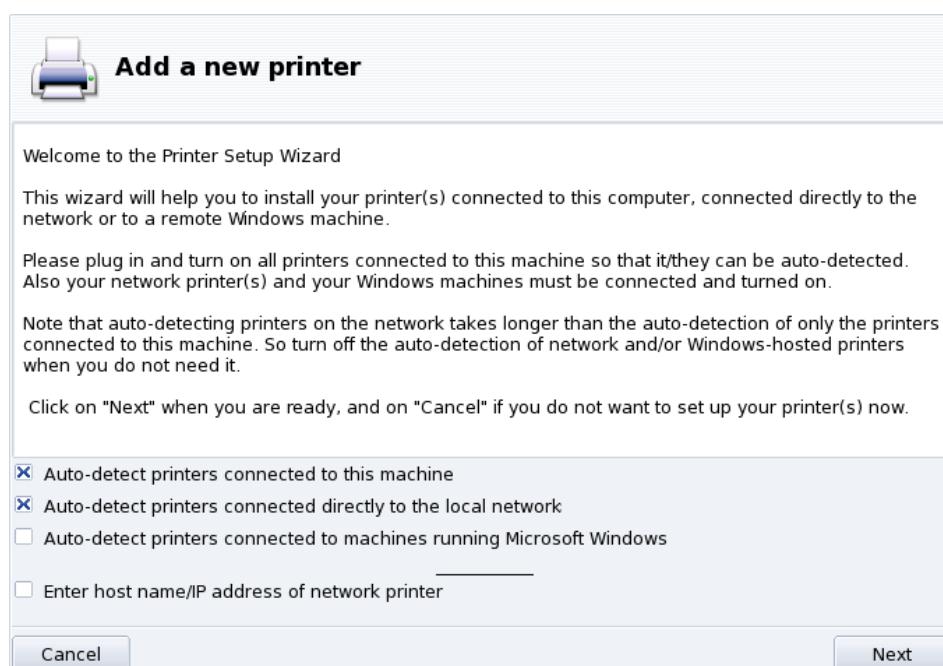
Figure 3-17. Printer Type

Specifying the Location. If you happen to know all parameters required to access a specific network printer, select Enter host name/IP address of network printer. Configuration steps are then similar to the ones involved in auto-detection procedure.

3.7.5.2. Choose the Printer
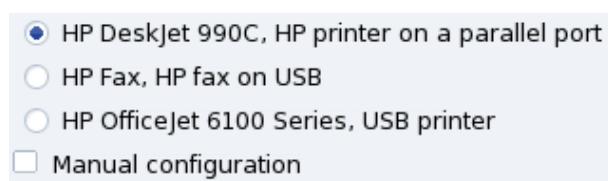
Figure 3-18. Detected Printers List

1. Choose the Printer to be Configured

   Select the printer you want to add from the list of detected printers. If the detected printer isn't the correct one check the Manual configuration box and proceed with the printer model step. If autodetection fails, remove the check mark from all check boxes, click on Next and follow the instructions below.

2. Specifying the Driver Manually

   PrinterDrake displays your printer's model name. Choose Select model manually if it's incorrect. Select the printer you have or a compatible one (see *Choose the Printer*, page 35) if yours is not specifically listed.

3. Manufacturer-Supplied Driver

   If you want to install the driver supplied by your printer manufacturer, click on the Install a manufacturer-supplied PPD file button and select the medium containing the PPD file and browse to it. Accept subsequent dialogs to use your chosen PPD file.

4. HP Multifunction Devices

   If you own a multi-function device such as those of HP or `Sony`, an information window pops up and gives you information about your scanner and scanner software (*Installing and Sharing Scanners*, page 39). Additional required packages are also installed.

   Fax Virtual Printer. If your device also provides fax functions, you are given an option to create a virtual fax printer that will actually queue the printed documents so they can be later sent via fax.

5. Optional Configuration Step

   If your printer has optional add-on devices (finishers, extra paper trays, etc.), you are asked which features are actually installed.

3.7.5.3. Printer Test

Several test pages are available (see figure 3-19). We recommend you print at least one test page so you can immediately correct the parameters if something is incorrect. The printer should begin to print almost immediately.

Figure 3-19. Testing the Printer

3.7.5.4. It's Done

If you're not satisfied with your test page, answer the appropriate question with No and you will be led to the printer configuration menu (see figure 3-20) where you can correct the settings. See *Reconfiguring an Existing Printer*, page 37.

Your printer will now appear in the list of available printers in the main window (see figure 3-14).

3.7.6. Reconfiguring an Existing Printer

Double-clicking on a printer's name in the list, or clicking on the Edit button, displays a menu where you can choose actions to take on the selected printer (figure 3-20). You can change the printer name, options, etc.
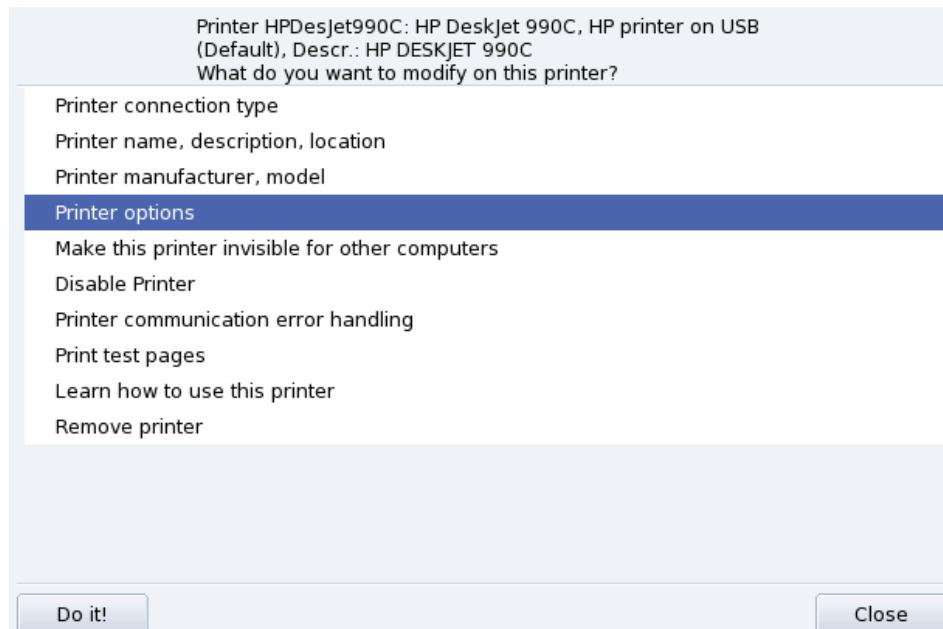

Figure 3-20. Modifying an Existing Printer

Here are some of the most useful entries:

- Printer name, description, location. If you have many printers around it is better to give them explicit names, and meaningful descriptions, plus a location so people don't end up looking desperately for their printouts in many floors.

- Printer Options. Shows the different options available for that printer (paper size, printout mode, etc.), so you can set a default value for them.

- Make this printer invisible for other computers. Printers are normally made available to other computers in the local network. Using this option you can disable this behavior for the currently selected printer.

- Disable Printer. Use this option to remove a printer from those to the system's users. You might need to temporarily disable a printer under maintenance so that users don't try to use it in the meantime. When a printer is disabled, that option changes to Enable printer.

- Learn how to use this printer. Displays information on how to use a particular printer model. In the case of a multi-function device from HP, additional information for the "extra" functions is also displayed.

- Remove printer. Deletes that printer's configuration from the system.

Select an action in the dialog and then click on the Do it! button to perform it.

3.7.7. Controlling Automatic Installations

Open the Options→Configure Auto Administration menu to go to the automatic installation options form.
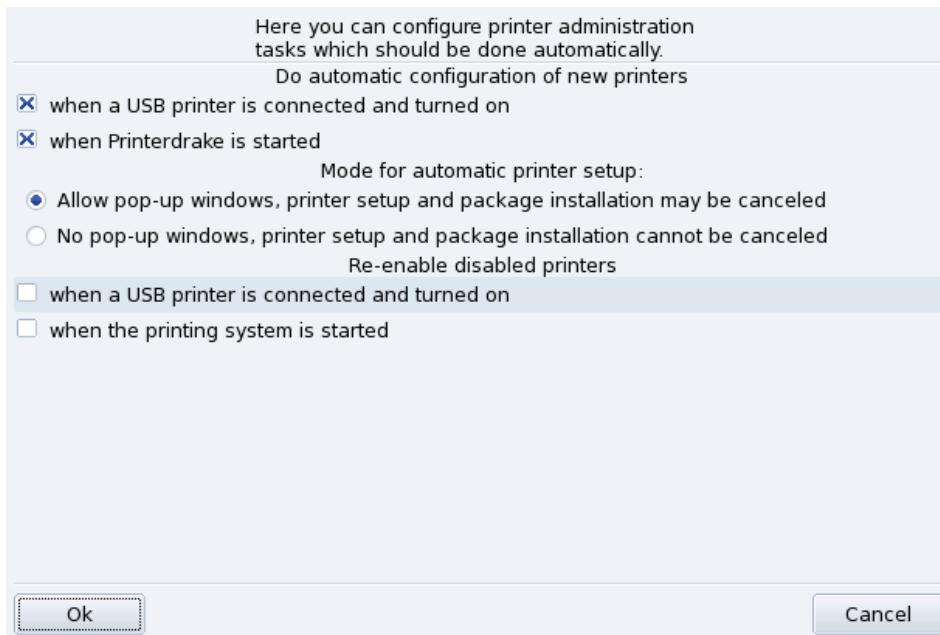
Figure 3-21. Set Automatic Installation Options

You can here configure whether new printers should be automatically detected, automatically configured, etc.

3.7.8. Expert Mode

The expert mode activates additional features in the application.

More Technical Installation Wizard. The installation wizard displays more technical information and allows you to configure printer name and other options directly from within the wizard.

Choose a Different Printer Driver. Different drivers are available for the same printer. In expert mode, a third level appears in the printer model selection list (see *Choose the Printer*, page 35) letting you change each printer's driver.

No Automatic Configuration. If PrinterDrake is in expert mode, it doesn't automatically configure new local printers on start-up. Use the Add printer button to configure the printer. However you can choose to Configure Auto Administration from the Options menu to override that behavior.

Automatic correction of CUPS configuration. This new option appears in the CUPS server configuration window (figure 3-15. It is activated by default. Leave the mouse over the option name to get more information about what it does.

3.8. Installing and Sharing Scanners

The ScannerDrake wizard helps you install your scanner. Make sure your scanner is powered on and launch ScannerDrake by clicking on the Scanners entry of the Mandriva Linux Control Center's Hardware section.

Tip: Please note that not all scanners are supported under GNU/Linux. Before buying new hardware, remember to check out Mandriva's Hardware Database (`http://hcl.mandriva.com`) and the SANE home page (`http://www.sane-project.org/`) for compatibility issues.

3.8.1. Main Interface and Scanner Installation

The program tries to detect your scanner's manufacturer and model. If it finds the scanner then information about it is displayed in the upper part of the wizard's main window. The window also offers a few action buttons (figure 3-22).
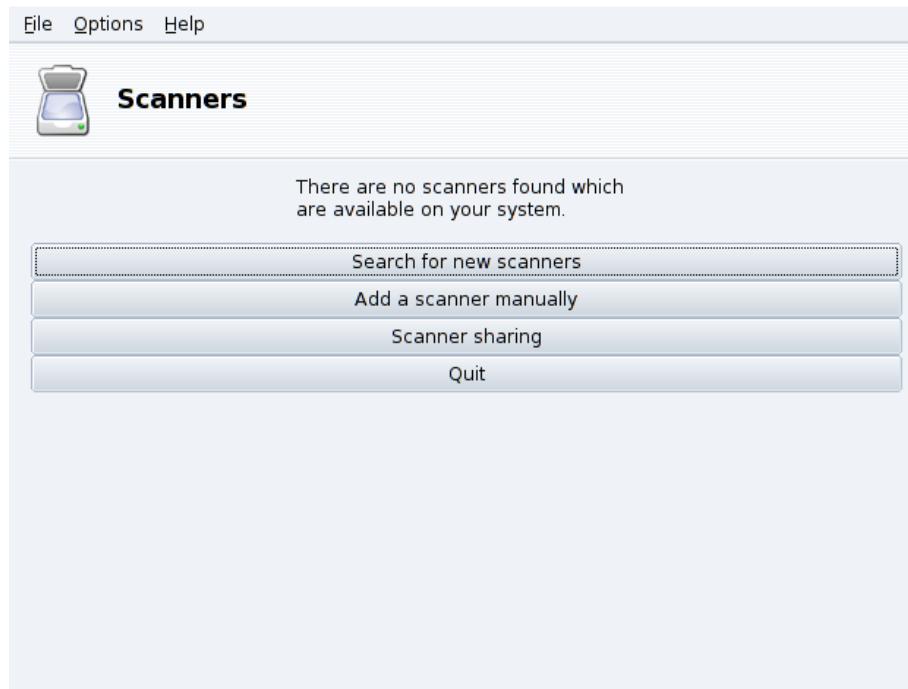

Figure 3-22. Installing your Scanner

Search for new scanners

> Click on this button to autodetect a new scanner you have just plugged in.

Add a scanner manually

> Use this button if the automatic detection fails and then look for the specific model you own by browsing through the list of available scanners and models.
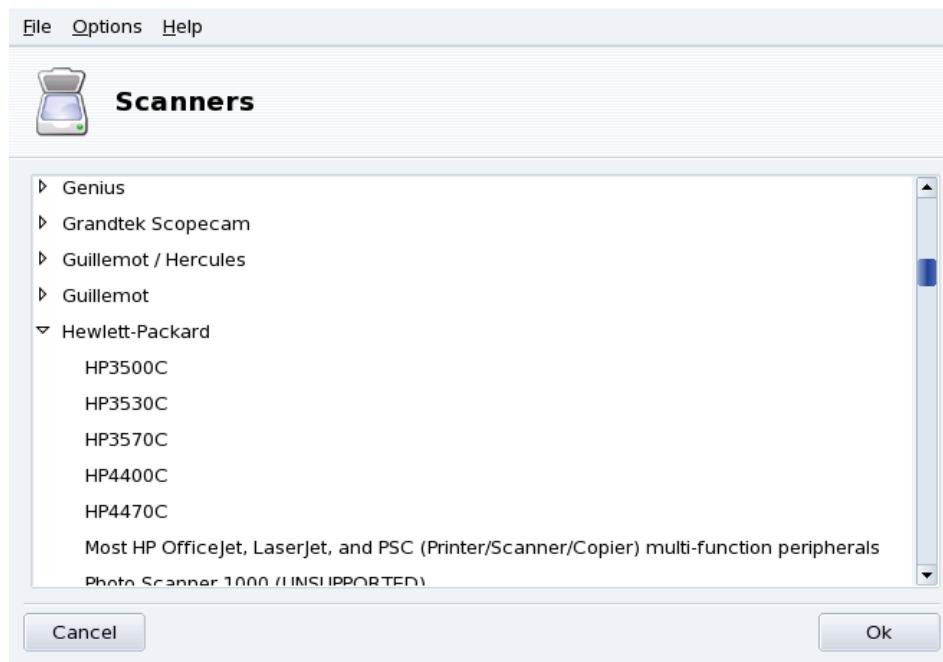
Figure 3-23. The Tree-list of All Known Scanner Models

Choose the right Port. After choosing the appropriate model, you can leave the default Auto-detect available ports option unless you have a parallel port scanner, in which case selecting `/dev/parport0` in the pull-down list should be the right choice.

HP multi-function devices

Note that HP multi-function devices, such as the OfficeJet and PSC printers, must be configured through Printer-Drake. Please refer to *Configuring Printers with PrinterDrake*, page 29. The scanning part of non-HP multi-function devices can be set up with ScannerDrake as a stand-alone scanner.

3.8.2. Share your Scanner

ScannerDrake allows for scanner sharing between users connected via a LAN.
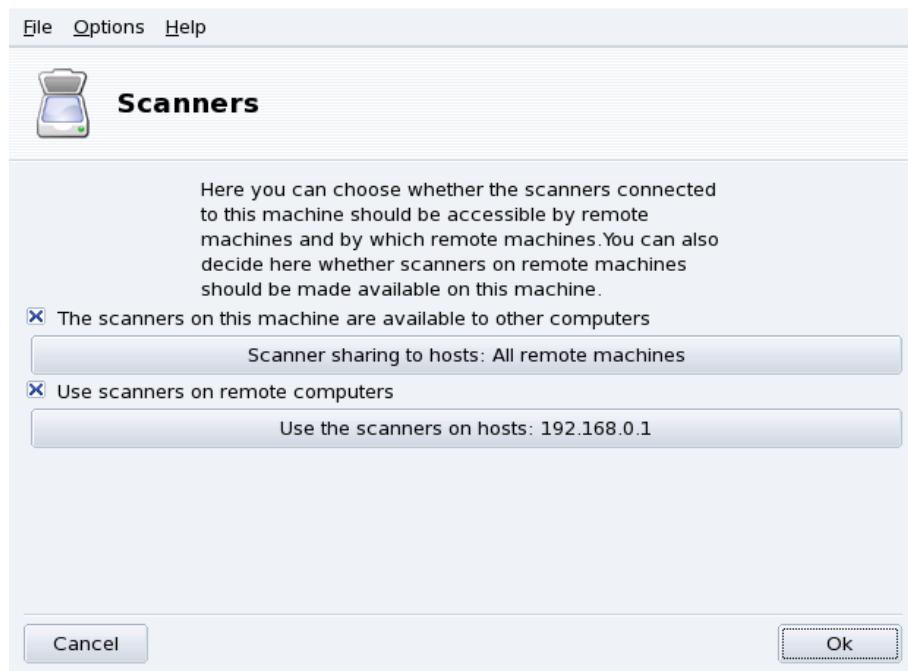
Figure 3-24. Sharing Scanners within a LAN

Share Your Own Scanner

1. Check the The scanners on this machine are available to other computers box.

2. Click the Scanner sharing to hosts button and then Add host to specify which hosts will be actually allowed to access your scanner.

Use Other People Scanners

1. Check the Use scanners on remote computers box.

2. Click the Use the scanners on hosts button and then Add host to specify which hosts serve the scanner you wish to use.

3.9. Setting up your UPS

 This tool will configure the NUT (Network UPS Tool) service for you. The service checks the UPS connected to your machine and automatically shuts it down when the UPS is about to run out of battery power.

**Automatic Installation.** Open the Mandriva Linux Control Center in the hardware section and click on Set up a UPS for power monitoring to launch DrakUPS. Check the Connected through a serial port or a USB cable button to let DrakUPS autodetect your UPS.

Manual Configuration (Serial Port)

1. Select the Manual configuration option.

2. Select your UPS from the list of manufacturers and models.

3. Then assign a Name, Driver, and Port[1].
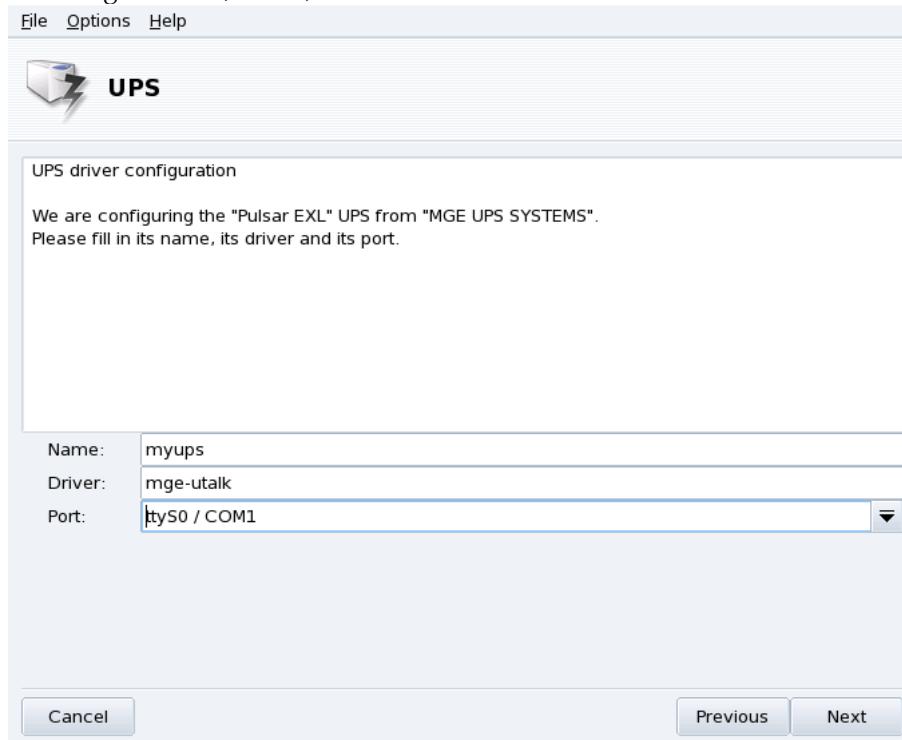
If all went well your UPS should now be configured and ready to help avoid bad power outage surprises.

---

1. The Name and Driver fields should automatically be filled. Of course, you can change its name but we recommend you keep the driver name.

Chapter 4. "Network & Internet" Section

4.1. Network and Internet Connection Management

Tip: Before connecting to the Internet, you are encouraged to set up a firewall on your machine so as to avoid bad surprises such as intrusions to your system. You can set up a very simple, yet effective, firewall using DrakFirewall. Please refer to *Securing your Internet Access via DrakFirewall*, page 88 for more information.

The drakconnect set of tools allows you to easily configure your network access, whether it be to the *Internet* or to a local network. Open Mandriva Linux Control Center and select the Network & Internet section to access drakconnect tools. A view of the main interface is shown in figure 4-1.
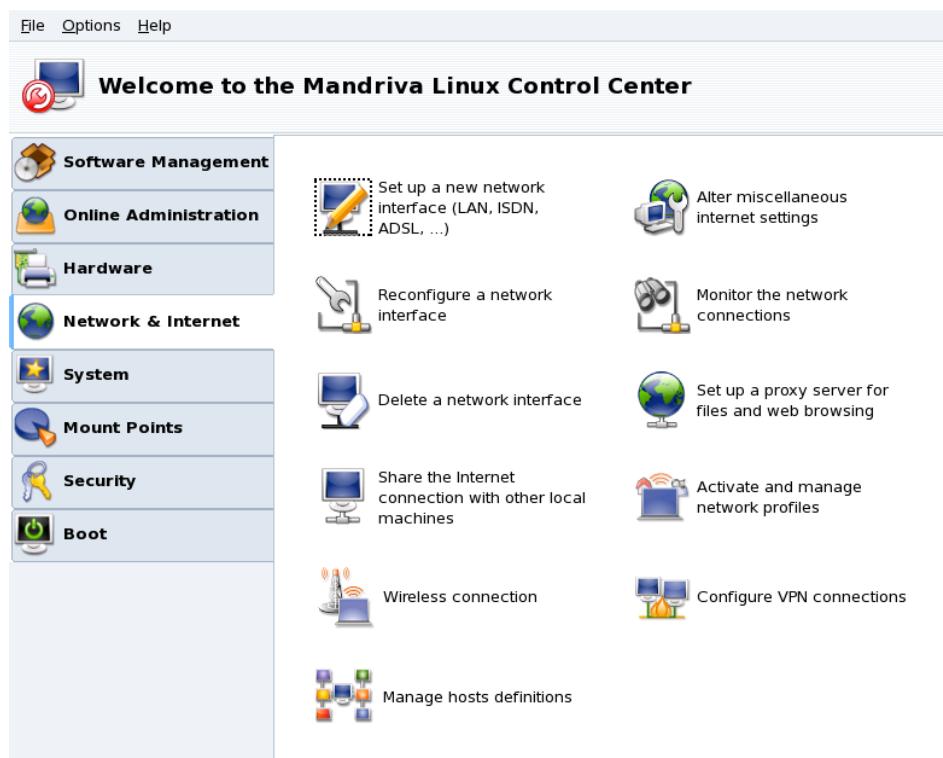

Figure 4-1. DrakConnect Tools

4.1.1. Set Up a New Network Interface

drakconnect supports different types of Internet and network connections. The first step consists of choosing which type of connection you wish to configure. Always make sure you have all the information provided by your ISP or network administrator at hand.

Note: After a connection has been configured it can be further modified using the Connections management interface (see *Reconfigure Interfaces*, page 48).

4.1.1.1. Wired Ethernet Connection

1. Select the Ethernet type

   Your NICs are detected automatically; if you have more than one, you have to select the one you wish to configure. You can also load a driver for your NIC manually.

2. Automatic or Static Configuration

   You now have to specify whether the network parameters are automatically set up (Automatic IP (BOOTP/DHCP)) or not (Manual configuration): fill the next steps with the parameters which your ISP or network administrator gave you. An example of the manual configuration of IP parameters is shown in figure 4-2.

3. Setting Parameters

   a.
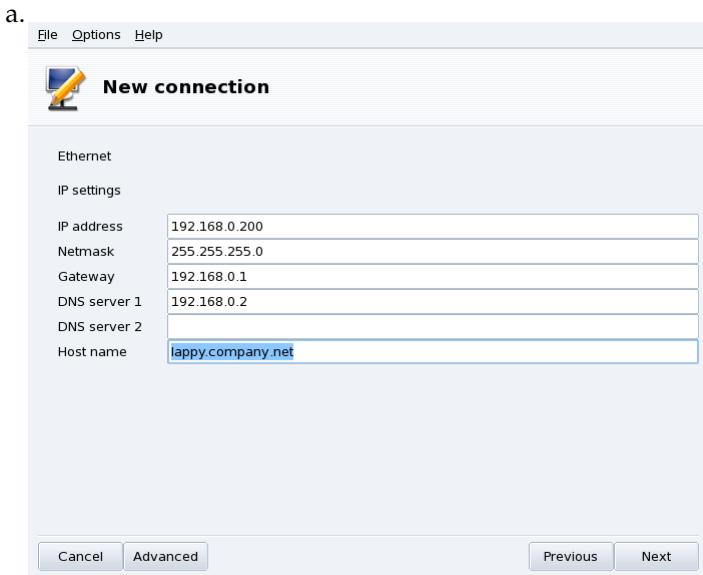
   If you chose the static IP configuration type, you have to specify the rest of the parameters, namely the hostname, DNS server IP address(es) and the IP address of the machine giving you access to the Internet, known as the gateway (see figure 4-2).

   b. Dynamic Configuration

   If you configure the network with DHCP you can optionally provide DNS server information (remove the check from the Get DNS servers from DHCP option and fill the corresponding fields with the IP addresses or hostnames of the DNS servers) and the machine's hostname (remove the check from the Assign host name from DHCP address option and fill the corresponding field with the hostname: this is the name which will be assigned to the machine when no network configuration has been found).

4. Connection Control

   Allow users to manage the connection

   If you wish users to be able to bring up or shutdown the connection without having to provide the `root` password (see *Monitoring Connections*, page 49) check this box.

   Start the connection at boot

   Uncheck this if you want the connection to be activated on demand only.

   The Net Applet: An applet appears in the desktop's panel indicating that the connection is up

   or down

   . Right click on it to access a menu that will also let you control the connection's state as well as other parameters.

4.1.1.2. Wireless Connection

This entry allows you to configure WiFi PCMCIA or PCI devices.

1. Choose WiFi Card

    If your card is not listed, choose the Use a Windows driver entry. The next step then asks you to select the driver from the manufacturer's card drivers CD.

2. Choose Network

    A list of detected networks is then shown. Select yours, or unlisted otherwise.

3. Wireless Settings

    Operating Mode

    > The mode the card will operate on, with respect to the other WiFi devices in the network. The most common one is Managed to simply connect to an existing access point.

    Network Name (ESSID)

    > The name of the network you wish to connect to. Ask your network administrator.

    Encryption Mode

    > This depends on the network settings, ask your network administrator.

    Encryption key

    > This also depends on the network settings, ask your network administrator for the key the network uses.

4. Network Configuration

    This is now similar to the traditional ethernet network setup: *Wired Ethernet Connection*, page 43.

5. Connection Control

    Check the Allow access point roaming box if you wish the connection to automatically switch from one access point to another, depending on the signal strength of it. Particularly useful when moving a laptop around.

Managing Connections. Consult *Wireless Connections Management (Roaming)*, page 54 to learn how to configure and manage various wireless networks.

4.1.1.3. DSL Connection

1. You are first asked which device your DSL modem is connected to, select it and click Next.

2. You then see a list of countries/ISPs. If yours is listed, select it: most of the following parameters will be automatically set. If your ISP is not listed, select the Unlisted - edit manually option, click on Next and fill the parameters with the settings provided by your ISP.

3. You have to specify the connection type, as advertized by your provider. The most common type being DHCP, followed by PPPoE and PPPoA.

Figure 4-3. Setting the ADSL Connection Type

4. All the protocol types need at least a user name and a password, fill the corresponding fields with them. The required packages are installed.

5. You are then asked whether or not to bring the connection up at boot. Since ADSL connections are of the "always up" type, you can safely select Yes. Finally you can test the connection: we strongly recommend you to do so, to make sure all parameters are accurate.

4.1.1.4. Cable Connection

This configuration is very similar to the one described in *Wired Ethernet Connection*, page 43. Make sure you have all required parameters provided by your ISP handy.

Authentication. Some cable ISPs need you to authenticate. If this is your case, select the Use BPALogin option. If you are unsure or don't know, it is safe to select the None option.

4.1.1.5. ISDN Connection

Simply make sure you select the right parameters in all steps, concerning your area and provider.

The last step gives you the option to handle the connection status through the net applet, this can prove useful if you only need the Internet connection from time to time.

4.1.1.6. Modem Connection (POTS)

1. A list of detected modems is shown. If no modem was detected then only the Manual choice option is shown, click on Next and choose the communications port the modem is connected to. The required packages are installed.

2. You then see a list of countries/ISPs. If yours is listed select it and continue to the next step: some parameters (connection name, phone number to dial, and authentication scheme) will be automatically set. If not, select the Unlisted - edit manually option.

3. Verify the parameters, add the missing ones provided by your ISP.
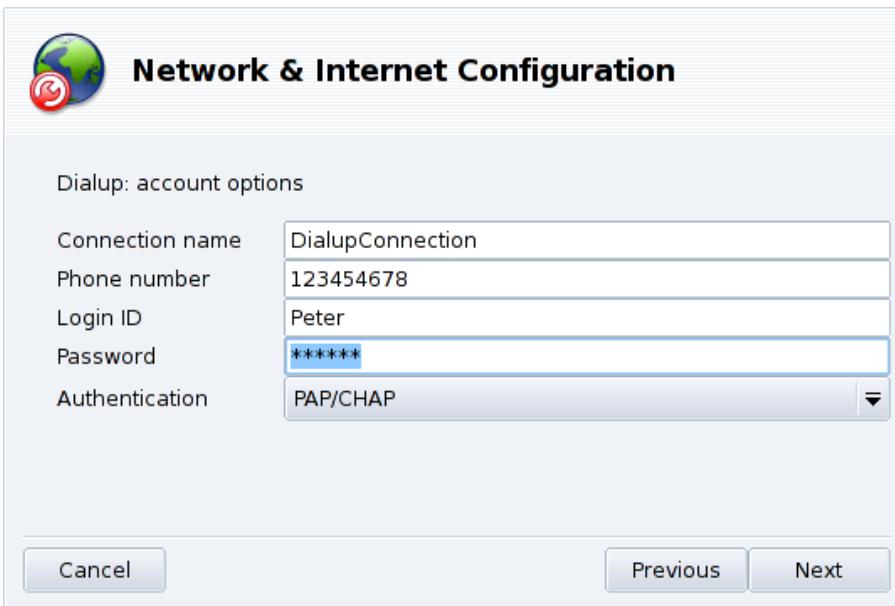
Figure 4-4. Entering Dial-up Connection Parameters

All parameters should be obvious, except for the authentication type. The value in the Authentication pull-down depends on what your ISP supports: Script-based (an old type of authentication method based on "expect" and "send" types of chat between your system and your ISP); Terminal based (a terminal window will pop up when the connection is made and you will have to login interactively); PAP, CHAP, or PAP/CHAP (authentication information exchange protocols, CHAP is preferred because it is more secure, PAP/CHAP will automatically choose the supported one).

4. Then come the IP, DNS and gateway settings. Nowadays, most ISPs provide them automatically when a connection is made, so selecting the Automatic option on them is usually a safe bet.

5. Connection Control

   Allow users to manage the connection

   You are then asked whether you wish to allow users to start the connection. That will allow them to do so without needing the `root` password.

   Start the connection at boot

   It is probably safer and cheaper to choose No.

6. Finally you are asked to test the connection: we recommend you to do so to make sure all parameters are accurate. You can now control your Internet connection using the net applet. You can also use the kppp remote access connection dialer (package kppp) by choosing Internet+Remote Access→KPPP from the main menu.

4.1.1.7. DVB Connection

This connection type is used for satellite connections.

1. Choose the connection card you wish to configure, and then the adapter settings.

2. Network configuration is then similar to the LAN connection type (see *Wired Ethernet Connection*, page 43).

4.1.1.8. GPRS/Edge/3G

This connection type supports Internet connections through cellular phone networks, accessed through a PCMCIA card. Third generation (3G) technologies, as well as older ones (GPRS/Edge) are supported. Support for newest HSDPA norm is also available.

4.1.2. Internet Settings
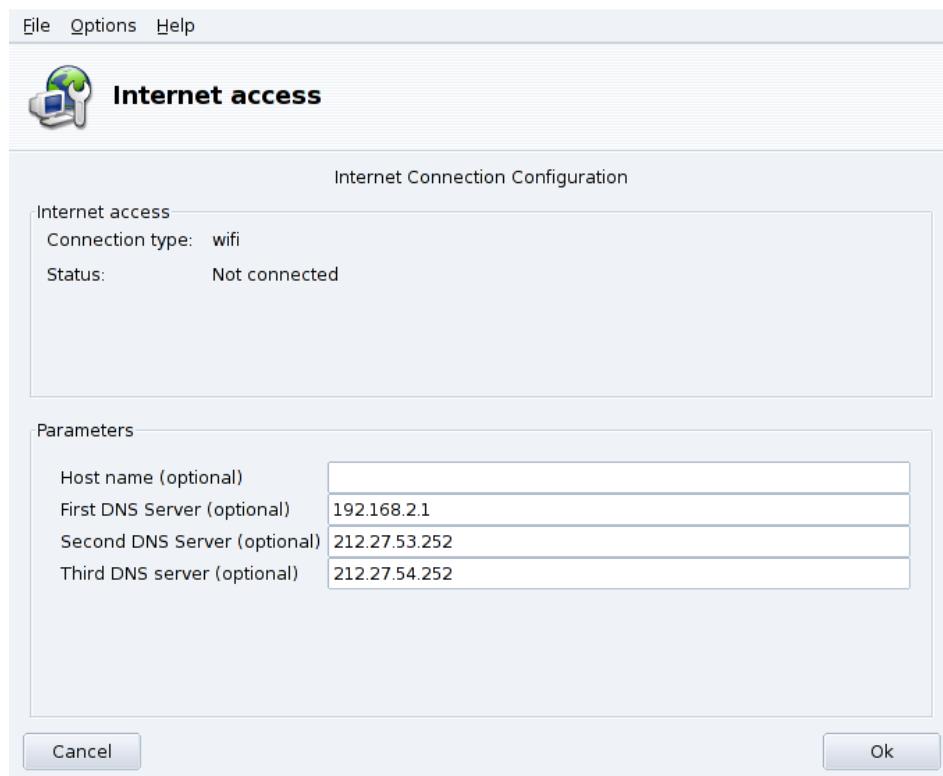
Figure 4-5. Configuring the Internet Access

This tool allows you to specify Internet access parameters if they need to be modified after your initial configuration. Please bear in mind that these parameters are system-wide and apply to all interfaces. To change the gateway address see *Reconfigure Interfaces*, page 48.

4.1.3. Reconfigure Interfaces
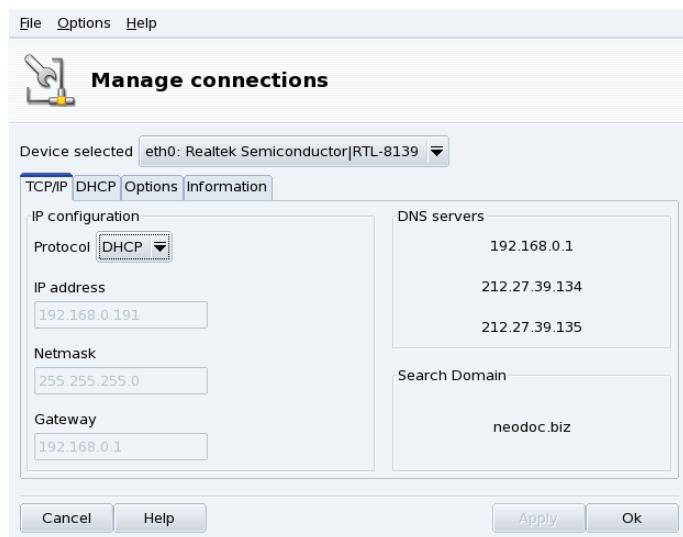
Figure 4-6. Manage Network Connections

This tool permits you to modify network interface-specific parameters, after you have set them up through the new interface wizard (see *Set Up a New Network Interface*, page 43). Use the drop-down list at the top to select the interface you want to configure. The tabs allow you to change parameters and options according to the network interface type selected.

4.1.4. Monitoring Connections
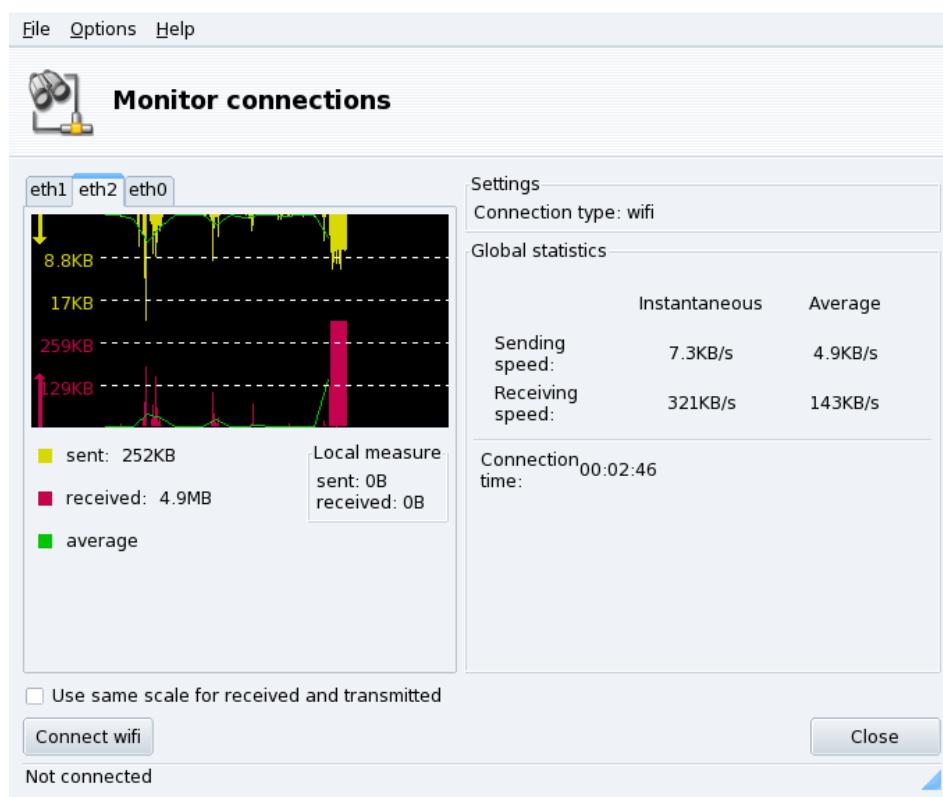
Figure 4-7. Real-Time Network Connection Monitoring

This tool shows the network interfaces activity. You can specify some options for the traffic graphic and statistics: update interval, scale, etc (see figure 4-7). It can also be used to control the status of the network connection, bringing it up or down using the button at the lower left.

Note: The network monitoring interface can be brought up by users through the net applet to monitor traffic.

4.1.5. Removing a Connection

This tool simply allows you to remove a network interface. Select the interface to be removed in the Net Device pull-down list.

> **Warning**
>
> You will not be asked for confirmation. Once an interface is selected for removal, pressing the Next button deletes it immediately.

4.1.6. Proxy Settings

If your Internet connections must (or can) pass through a proxy, this tool allows you to define the hostnames or IP addresses of proxies for the FTP and HTTP protocols. Fill the fields with the required values and click OK.

What's a Proxy. A proxy is a server which retrieves information from the Internet on your behalf, keeping a local copy of the web pages which are most frequently requested. They are referred to as "caching proxies", and optimize bandwidth usage. In some organizations, you cannot access the Internet directly. You must pass through a proxy which authenticates you before allowing you to connect to the Internet. This is usually combined with a firewall which only guarantees the proxy direct access to the Internet. They are referred to as "authentication proxies". In corporate or business environments, proxies perform both caching and authentication functions for performance and security reasons.

4.2. Activating and Managing Network Profiles

Mandriva Linux Control Center profiles enable you to store different configuration sets for your machine, for example for different locations. This is especially useful for laptops which need a different configuration for home, at the office, the coffee shop, etc. The parameters that can change from one profile to another are:

Network Configuration

    Activate different interfaces, with different configuration, for wireless for example.

Services Configuration

    Allows you to activate different services from one profile to another, for example a firewall at home and no firewall at the office (see *Configuring Start-Up Services*, page 57).

4.2.1. Profile Handling

New profiles you wish to create are based on the active one. All modifications are automatically recorded in the active profile. A single menu (Profiles) lets you manage them.

Figure 4-8. The Control Center Profiles Interface

Activate

> Make the selected profile active.

Clone

> Creates a new profile based on the selected one's settings. A dialog pops up asking for the name of the new profile. Don't forget to activate that profile after creating it if you wish to configure it.

Delete

> Deletes the currently selected profile, without further prompts. Please note that a warning is shown if you try to delete the active profile, because it cannot be removed while being used.

The default Profile. This is the profile that will be used at boot time. It cannot be deleted.

Example: Create a New Profile for your Dial-up Home Connection. You come back home with your brand new laptop which your system administrator configured so you can connect to your corporate network. You now want to configure the network to access the Internet from home with a dial-up connection.

1. Create a new profile called "Home".

2. Switch to it.

3. Reconfigure your network so that the modem, instead of the network card, is used to access the Internet (see *Network and Internet Connection Management*, page 43).

4. Connect to the Internet.

5. When back at the office, switch back to the "default" profile.

4.2.2. Choosing a Profile at Boot Time

It's more convenient to specify a profile at boot time than to activate it once the system is booted. drakboot (*Changing your Boot-up Configuration*, page 93) allows you to associate a specific profile to each menu entry of the bootloader.

Label	linux-Home
Image	/boot/vmlinuz
Root	/dev/hda5
Append	resume=/dev/hda6 splash=silent
☐ Default	

Video mode	800x600 16bpp
Initrd	/boot/initrd.img
Network profile	Home

Ok	Basic		Cancel

Figure 4-9. Associating a Profile to a Boot Entry

Create or modify a boot entry in drakboot. In the Advanced options, access the Network profile pull-down menu and select the profile you want to associate to it.

4.3. Internet Connection Sharing

This tool configures your system so that it acts as a gateway to the Internet for other machines connected to it via a LAN. This is very useful at home for example, if you wish all computers to access the Internet through the same Internet link.

Local Network (wireless or cabled)

The Internet

Other local machines

Your machine (gateway)
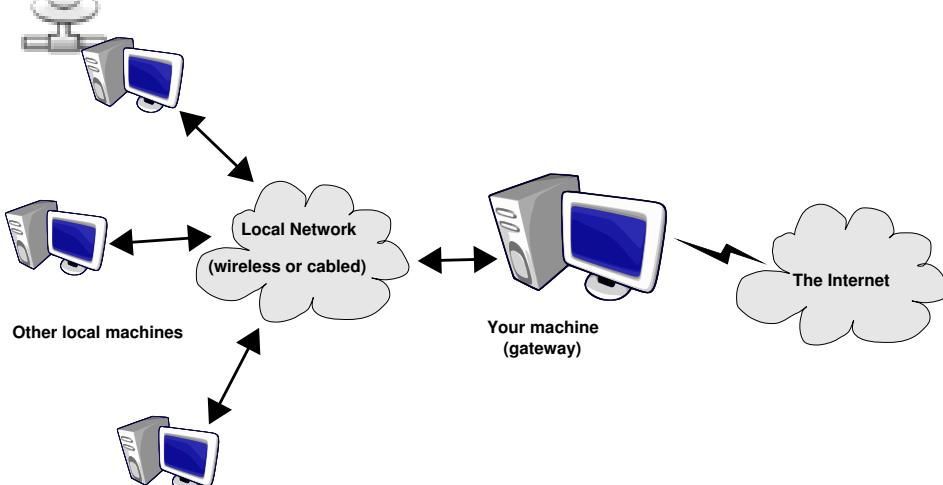
Figure 4-10. A Simple Gateway Configuration

The overall procedure is the following:

1. Configure your Internet access (*Network and Internet Connection Management*, page 43). In order for your machine to act as a gateway, you need an already configured and working connection to the Internet, plus a network connection to your LAN. This implies at least two interfaces, for example, a modem and an Ethernet card.

2. Setup the gateway (*The Gateway Connection Wizard*, page 53).

3. Configure the other local machines as clients (*Configuring the Clients*, page 54).

Warning

This wizard also configures a firewall to block most connections from the Internet. You are encouraged to check that the firewall configuration (*Securing your Internet Access via DrakFirewall*, page 88) suits you after completing the wizard.

After you complete this wizard, all computers on the LAN will be able to access the Internet. Their configuration will be automated due to the DHCP server which is installed on your gateway, and the web access will be optimized due to the use of the Squid transparent proxy cache.

4.3.1. The Gateway Connection Wizard

These are the steps that the wizard takes:

1. Choosing the Internet Interface

   You first need to specify the name of the interface connected to the Internet. Make sure you select the correct one from the drop-down list. It should be the interface name you configured in the Internet Configuration Management tool.

2. Choosing The LAN Network Adapter

   If you have more than one Ethernet interface, and depending on what you chose as your Internet interface, the wizard might ask you to select the one connected to your LAN[1]. Make sure you select the correct one.

3. Local Area Network Settings
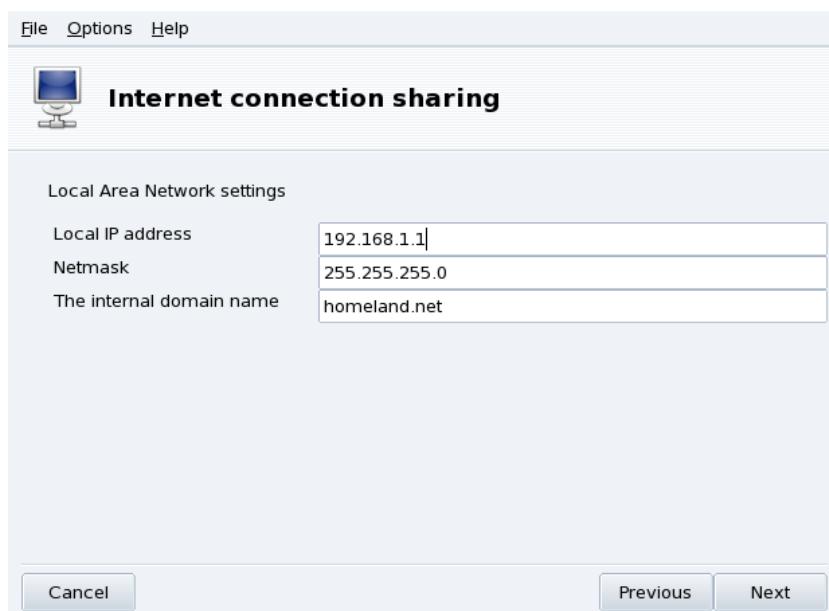
Figure 4-11. Configuring The LAN

At this point, if it is the 1st time the system has been configured as a gateway, the wizard proposes default parameters for the new local network to be managed. Check that these values are not already in use in your network, and proceed to the next step.

Otherwise, the wizard will first offer to reconfigure the LAN interface so that it will be compatible with the gateway services. It is recommended that you leave the default options and click on Next. Then, all the required software is installed.

4. DNS Configuration

---

1. Note that all traffic to and from this network passing through the gateway will be masqueraded, that is: it will appear (from an Internet point of view) to come from the gateway instead of from the LAN.

If you plan on having a local name server on your machine, you can check the box. Otherwise you can choose to use the name server of your provider. If you don't know what a name server is, leaving the box checked is safe.

5. DHCP Server Configuration

   Installing a DHCP server on your machine will allow all client machines to have their network configuration automatically done. Otherwise you will have to configure each of the clients by hand: IP address, network, gateway, DNS.

6. Proxy Caching Server (SQUID)

   A caching server records the Internet pages requested by local browsers. Then if the same page is asked for again by someone else, it is able to serve it without needing to retrieve it again from the Internet, thus saving bandwidth, and improving response time. This is very useful if there are many clients behind the gateway.

   The application used to perform this task is Squid (`http://www.squid-cache.org/`).

When the wizard is completed, any required packages are installed and configured.

> **Disable Connection Sharing:** The next time you launch this wizard, the first step proposes either to reconfigure or to disable connection sharing.

4.3.2. Configuring the Clients

Configuration of the clients mainly depends on whether you chose to install a ***DHCP*** server on your gateway or not. By configuring the clients on the local network to use DHCP, they will automatically use the Mandriva Linux machine as a gateway to the Internet. This works for Windows®, GNU/Linux and any other OS which supports DHCP.

If you have no DHCP server, you have to configure each of your machines manually, according to the network parameters set on the connection sharing wizard.

For DHCP, on a Mandriva Linux client system, make sure you selected DHCP in the Protocol pull-down list when configuring the network as shown in figure 4-12.
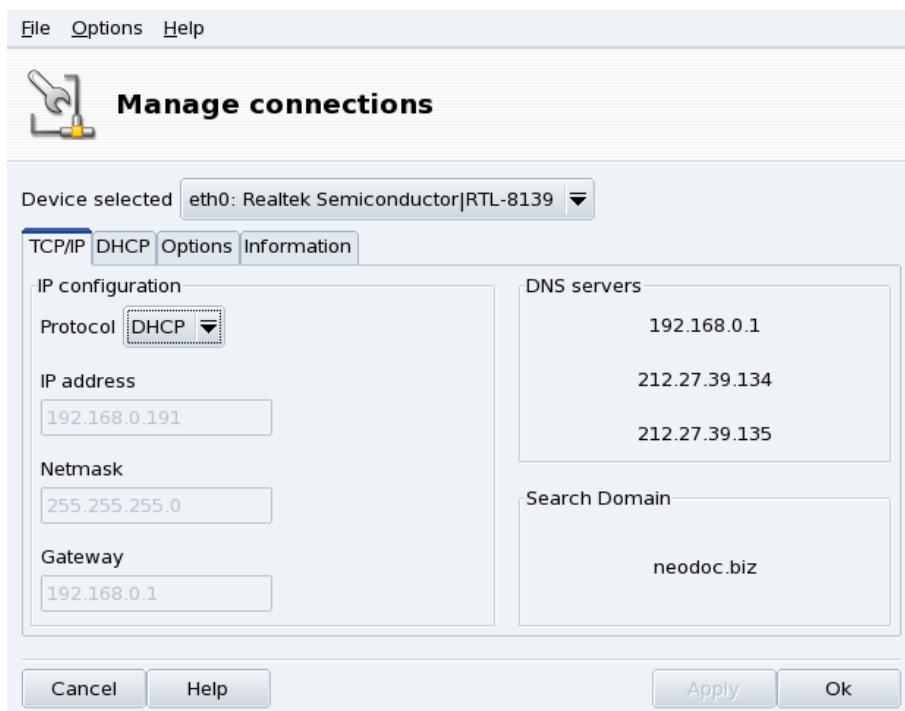

Figure 4-12. Configuring a Client to Use DHCP

4.4. Wireless Connections Management (Roaming)

This tool shows the wireless networks currently available and allows you to switch between them, and to change their configurations. If you haven't configured your wireless interface yet, please refer to *Wireless Connection*, page 44 for information. figure 4-13 shows DrakRoam's interface: a list of the available networks, together with their status, and buttons for actions at the bottom.

Tip:

You can also right click on the "signal meter" icon in the panel and choose Manage wireless networks, then enter root's password, to access the tool.


Figure 4-13. DrakRoam Interface

4.4.1. Switching Networks

To change networks, select one of those from the list, then click on Connect. If the network is public you will be immediately connected. If the network is private, then you are asked for configuration parameters with the same dialog shown in figure 4-14. Provide required settings (in particular, the encryption key) and click Ok. Settings take effect immediately.

4.4.2. Configuring a Wireless Connection

If you need to change the network parameters, just select the network from the list, then click on Configure. See figure 4-14 for an example of a secured wireless network connection.

Figure 4-14. Changing Wireless Network Configuration

Make your adjustments and click Ok, the settings take effect immediately.

Chapter 5. "System" Section

5.1. Configuring Start-Up Services

At boot time, the system starts a number of services (programs which run in the background to perform a variety of tasks). This tool gives the administrator control over those services. See the *The Start-Up Files: init sysv* chapter of the *Reference Manual* for more information.

Figure 5-1. Choosing the Services Available at Boot Time

For each service, this is the list of items found in each column:

- Service name;
- Current Status: either `running` or `stopped`;
- Info: click on this button to get a little explanation about that service;
- On Boot: check this box if you wish this service to be automatically started at boot time[1]. Alternatively, if xinetd is installed and the service is a xinetd service, the label Start when requested will be displayed. Checking the box will then mean to activate that service in xinetd. You will also have to make sure that the xinetd service itself is activated.
- Start: immediately starts the service, or restarts it (stop+start) if it is already running;
- Stop: immediately stops the service.

After pressing the Start or Stop buttons, a tool tip shows you the status of the operation.

---

1. Generally in *runlevels* 3 and 5.

5.2. Managing Fonts on your System with DrakFont

This system sdministration tool enables you to review the different font families, styles, and sizes available on your system. It also allows for fonts to installed or removed.

The main window (see figure 5-2) shows a visual appearance of the currently selected font combination.
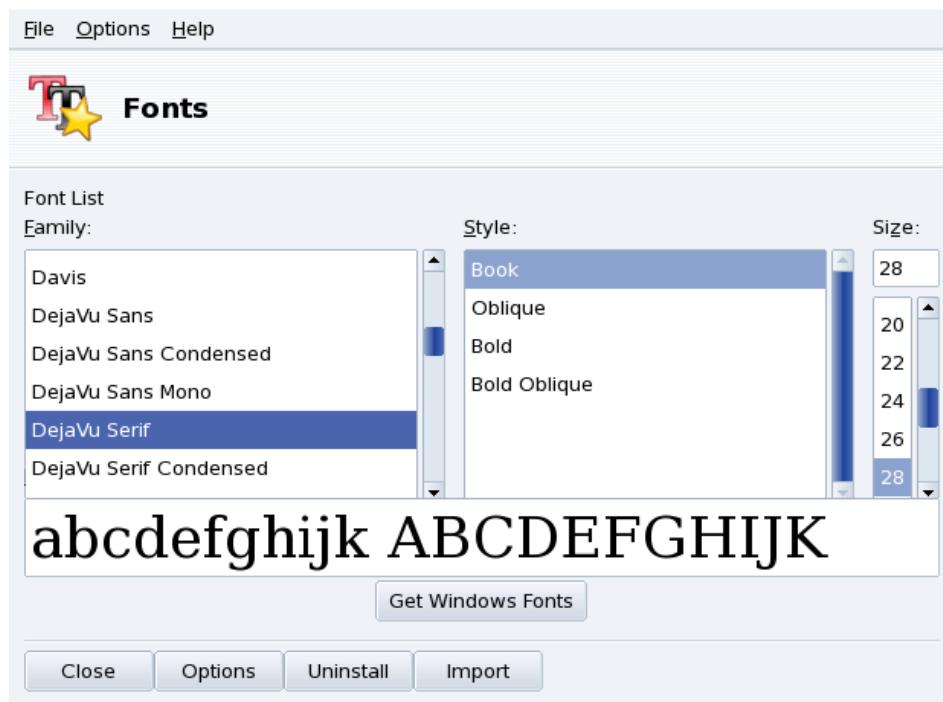
Figure 5-2. DrakFont's Main Window

drakfont is made up of a number of dialogs which are accessible through the buttons located at the bottom.

Get Windows Fonts

This button automatically adds fonts found on your Windows® partitions, if any, of your local hard drives.

Options

Allows you to specify which applications and devices (such as printers) will support the fonts. Select the ones you want support for and click on the OK button.

Uninstall

Allows you to remove installed fonts, in order to save space for example. Use this with great care, it could have side effects for your applications. In particular you should not remove fonts you did not install yourself.

This actually removes all fonts found in a given directory. Note that fonts manually added through drakfont are found in `/usr/share/fonts/drakfont/`

Import

Allows you to manually add fonts found outside the Mandriva Linux distribution, from a fonts disk you have purchased or from the Internet, for example. Supported font types are `ttf`, `pfa`, `pfb`, `pcf`, `pfm`, `gsf`. Clicking on the Add button will open a standard dialog allowing you to specify the font file to import. Once you've specified all the fonts you want to import, click on the Install fonts button.

> **Selecting more than one font:** To select more than one font, press the **CTRL** key while selecting the fonts you want to install and click OK, they will be added to the Import Fonts window. Then, click on the Install fonts button.

Note: When adding or removing fonts, the change might not appear immediately in the fonts list. Close and re-launch drakfont to ensure your changes were taken into account.

5.3. Setting your Machine's Date and Time

This little tool enables you to set your system's correct internal date and time.
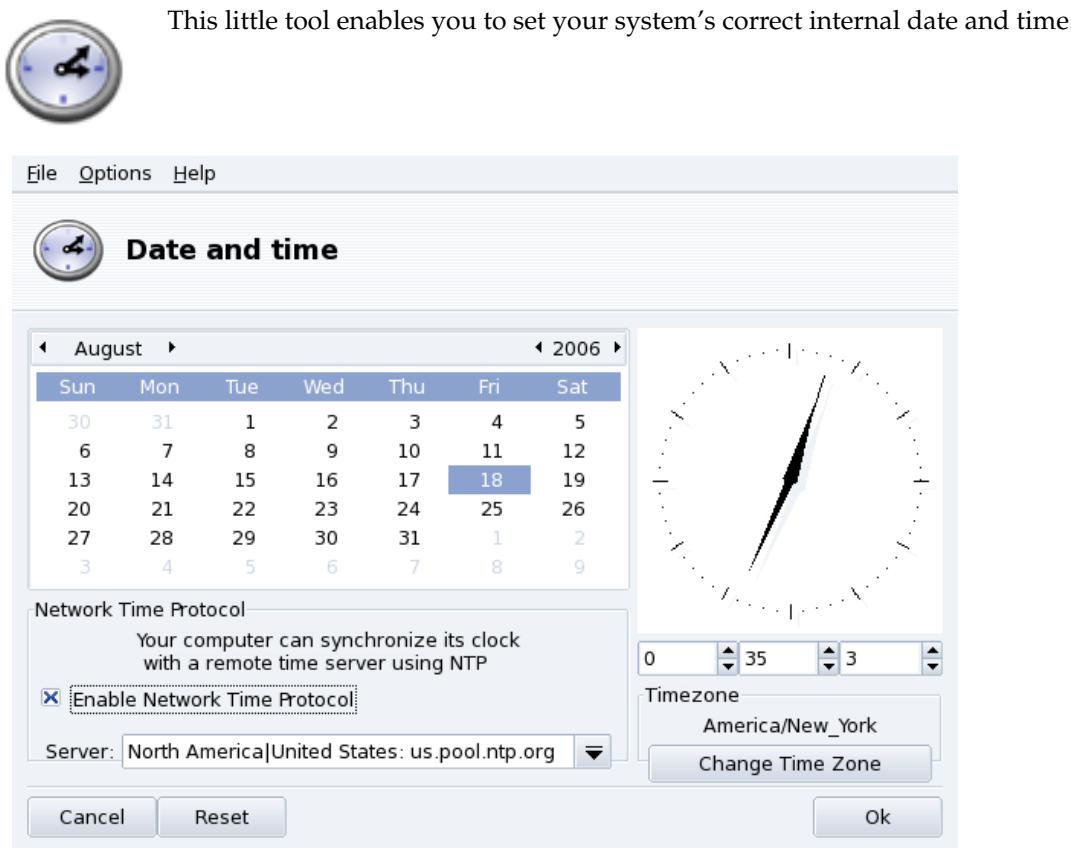
Figure 5-3. Changing Date and Time

You can set the date on the left and the time on the right:

1. Date

   To change the year, click on the little arrows on each side of the year; same procedure to change the month. This updates the month view where you can click on the current day in order to highlight it.

2. Time Zone

   We recommend that you check the time-zone settings for your geographical location. Click on the Change Time Zone button and select the correct place in the tree view.

   Once you've chosen the time zone, a dialog appears asking you whether your hardware clock is set to GMT. Answer Yes if only GNU/Linux is installed on your machine, No otherwise.

3. Time

   To change the time, you can either move the hour, minute and second hands of the analog clock, or change the numbers below it.

4. Automatic Clock Synchronization

If you have a permanent Internet connection and want your system to synchronize its internal clock with time servers on the Internet, put a check mark in the Enable Network Time Protocol option and select a server in the Server pull-down list, preferably one near you. If you know the name or the IP address of a local server you can also enter it manually in that field.

When you're finished, click on OK to apply your settings or Cancel to close the tool, which will discard your changes. If you want to return to your previous settings, click on Reset.

5.4. Monitoring System Activity and Status

This tool allows you to look for specific entries in various log files, therefore making it easier to search for particular incidents or security threats.

Additionally a nifty wizard allows you to set up mail alerts to warn you whenever the load is too high on your machine, or when a service is down.

5.4.1. Browsing System Logs
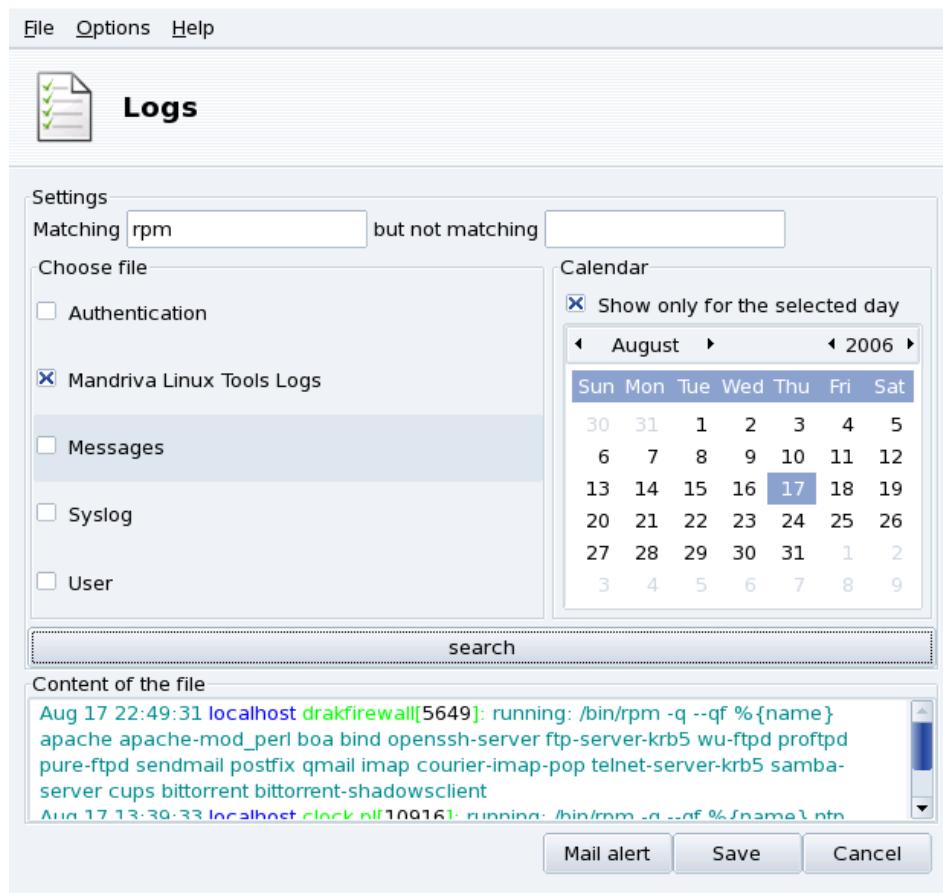
Figure 5-4. Browsing and Searching through System Logs

These are the steps to follow in order to browse or look for a specific event into the system logs:

1. Matching Terms

   You must choose which specific words to match by filling the Matching (log files contain the words) field and/or the but not matching (log files which don't contain the words) field. At least one of the two fields must be filled.

2. Log File

    Then in the Choose file area select the file you want to perform the search on. Simply check the corresponding box.

    > **Note:** The Mandriva Linux Tools Log is filled by Mandriva Linux-specific configuration tools, like those you find in the Mandriva Linux Control Center. Each time these tools modify the system configuration they write to this log file.

3. Date of Event

    Optionally, you can restrict the search to a specific day. In that case, check the Show only for the selected day box and choose the desired day from the calendar.

4. Search

    When all is set up, click on the Search button. The results appear in the Content of the file area at the bottom.

Clicking on the Save button opens a standard dialog letting you save the search results into a plain text (`*.txt`) file.

5.4.2. Setting up Mail Alerts

In order to facilitate server monitoring, Mandriva Linux supplies a simple tool which sends automatic mail alerts whenever something goes wrong on your server.

Clicking on the Mail alert button of the LogDrake main interface (see figure 5-4) starts the wizard. First you're asked whether you wish to configure or stop the mail alert system. Choose Configure the mail alert system entry in the pull-down list, and click Next.
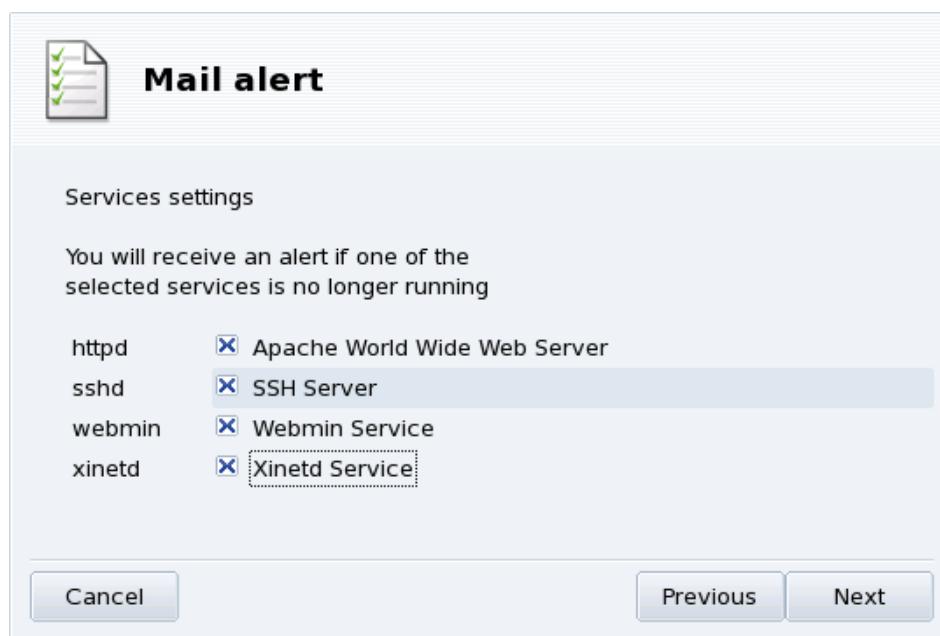

Figure 5-5. Setting up a Mail Alert: Services

The next step (figure 5-5) allows you to select the services you wish to receive alerts about if they stop working. Simply check the service boxes which interest you.

> **Note:** The services listed are the ones present on your system. Here's a list of the currently trackable ones:
>
> • Postfix Mail Server;

- Webmin Service;
- FTP Server;
- BIND Domain Name Resolver;
- Apache World Wide Web Server;
- SSH Server;
- Samba Server;
- Xinetd Service.

Figure 5-6. Setting up a Mail Alert: Load

Select the load you which you consider unacceptable by moving the Load slider (figure 5-6). A high system load may indicate that a process has gone out of control, or simply that there's a very high demand on this machine. Therefore a service is suffering from it and is delayed. As a rule of thumb, the load on your computer should not exceed 3 times the number of processors you have on it.

Figure 5-7. Setting up a Mail Alert: Recipient

Finally you need to tell the system to whom these alerts should be sent (figure 5-7). Provide an e-mail address and the mail server (local or on the Internet) to relay the alerts to.

When the wizard is finished, an hourly check is set up to verify services availability and the system's load. If needed a mail alert is sent to the alerts' recipient until the problem is solved.

5.5. Access to the Console

This tool simply opens a virtual terminal console for the `root` user. You can use it to issue any command, but be careful! There are no restrictions on the actions you can take on your machine as `root`, and you could render your machine unusable.

To learn how to use the command line interface, you should read the Introduction to the Command Line chapter of the Mandriva Linux *Reference Manual*. To exit the console, type `exit` or press the **Ctrl-D** keys.

5.6. Managing Users and Groups

UserDrake allows system administrators to easily add and remove users from the system, to assign users to a group, and to manage user groups in the same manner.

> **Note:** In this section we will only focus on user management. Group management being similar.

5.6.1. The Interface

Launching UserDrake will display the main window (figure 5-8) which lists the users currently defined on the system. You can switch from users to groups by clicking on the Groups tab next to the Users tab.
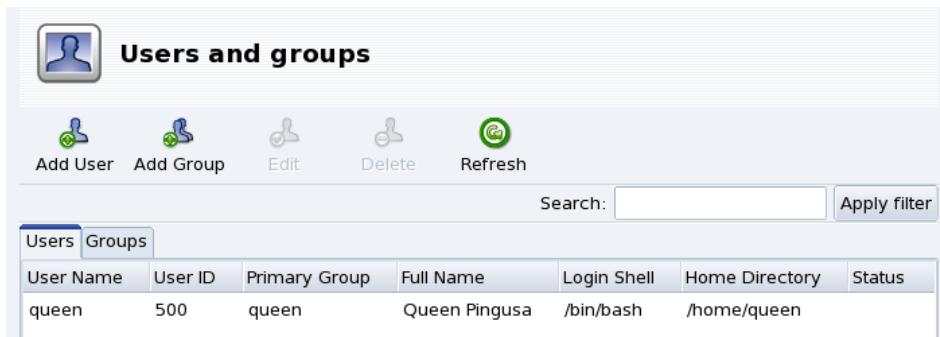
Figure 5-8. The User List in UserDrake

All changes have immediate effect on your local user database. If the user list is modified outside of UserDrake, you can refresh UserDrake's window by clicking on the Refresh button.

> **Note:** If you make changes to an already logged in user, those changes won't take effect until the next time he or she logs in again.

Available actions are:

Add User

Adds a new user to the system. We will detail this procedure in *Adding a New User*, page 64.

Add Group

Adds a new user group to the system.

Edit

Allows you to change the parameters of the selected user or group. We will detail editing user parameters in *Adding a New User*, page 64. In the case of a group you will be able to assign or remove users from that group.

Delete

Removes the selected user or group from the system. A confirmation dialog will be shown, and in the case of a user you will also be able to remove the user's `/home` directory and `mailbox`.

5.6.2. Adding a New User

We created the non-privileged user Queen Pingusa at installation time, and now we want to create a new user called Peter Pingus. Then we want to make them both members of the `fileshare` group, so that they can share folders with other users on the network .

Click on the Add User button, a dialog box to add a new user will pop up (see figure 5-9). The only required field is Login although we strongly recommend that you set up a password for this new user: enter it in both the Password and Confirm Password fields. You can also choose to add a comment in Full Name. Generally, this is the full name of the user, but you can put whatever you want.
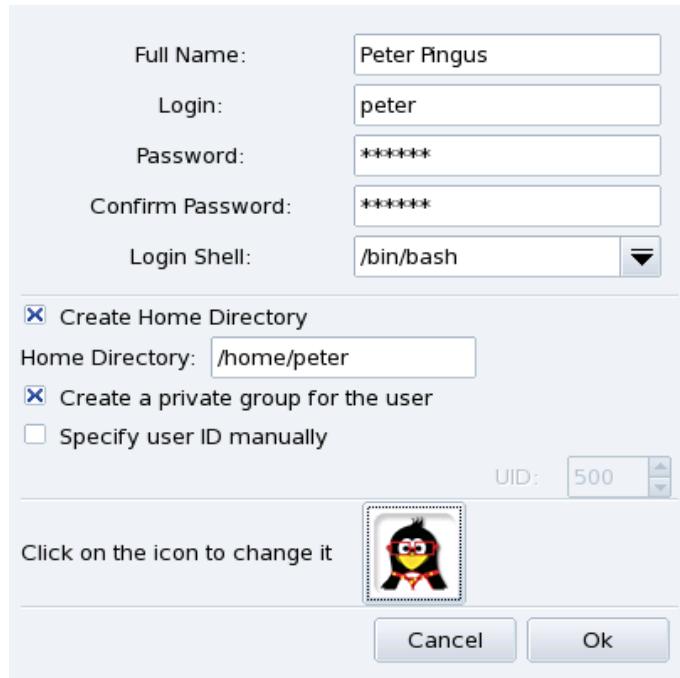
Figure 5-9. Adding a New User in the System

We now have two users in our list. Select one of them with your mouse, and click on the Edit button. The dialog box shown in figure 5-10 will pop up. It allows you to modify most available user parameters.
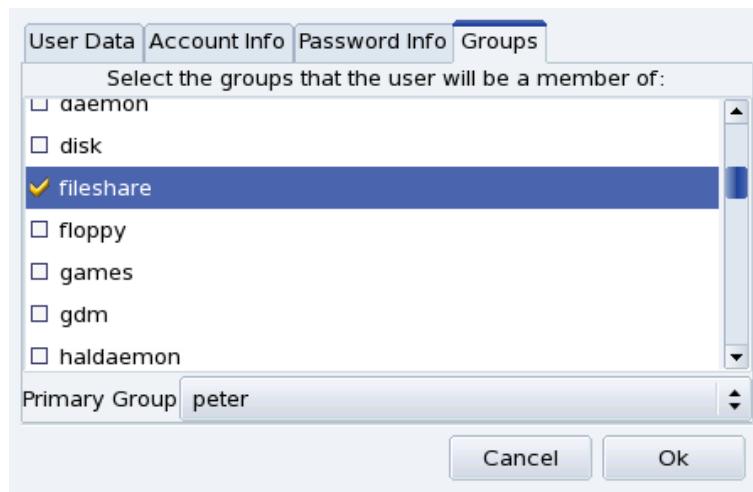
Figure 5-10. Adding Users to a Group

The dialog is made of the following tabs:

User Data

　　Allows you to modify information provided when the user was created.

Account Info

　　Enables you to provide an expiration date for that account, after which the user won't be able to connect to the system. This is useful for temporary accounts. It's also possible to temporarily lock an account to prevent a user from logging in. Finally, this tab allows you to change the icon associated with the user.

Password Info

　　Allows you to provide a password expiration date, after which the user will be required to change his password.

Groups

　　Shows the list of available groups where you can select the groups to which any user should belong.

For our users we just need to look for the `fileshare` entry and check the box associated to it. Then click on the OK button to make the changes effective.

5.7. Backing Up and Restoring your Files

This tool allows you to back up data present on your computer onto different media and also to a remote machine over a network. It also supports multiple profiles for different backup scenarios. Once the parameters are set, you can run the backup periodically. Then, you can forget about it until you wish or need to restore files.

5.7.1. A Practical Example Using the Wizard

You can access this tool by clicking on the Backups icon in Mandriva Linux Control Center's System section. Click on the Wizard Configuration button to start the wizard. After making your choices in each step click on Next.

#### 5.7.1.1. First Step: What to Backup
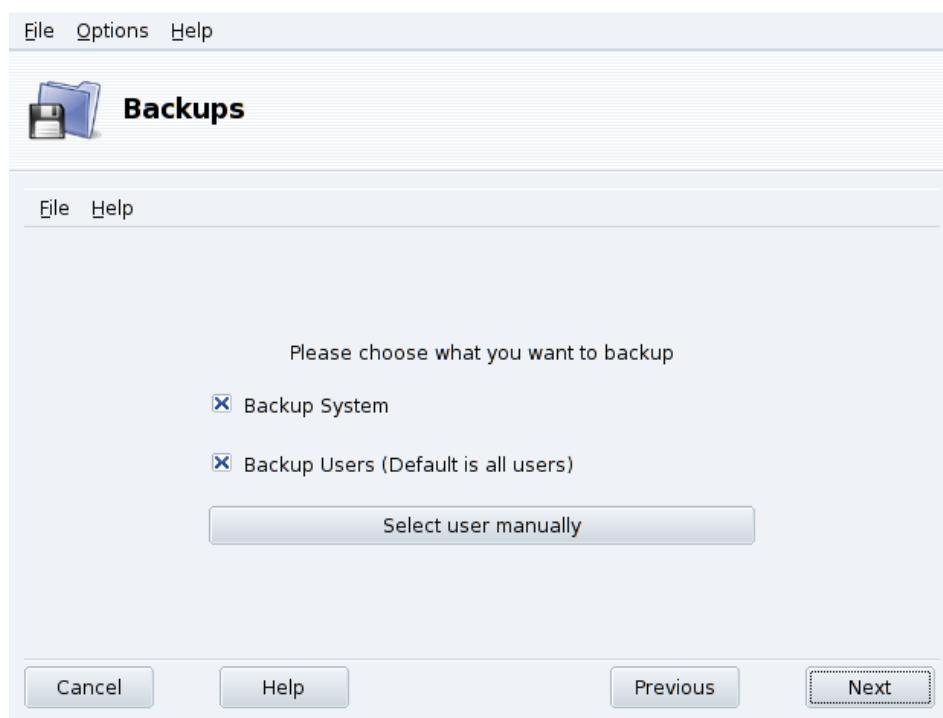
Figure 5-11. Selecting What to Backup

Select Backup System to include the `/etc` directory where all your current system configuration files lie. This allows you to "transport" your system to a different computer with little effort: only hardware-dependent configuration will have to be revised.

> **Note:** The "system" backup does not include applications themselves (i.e. executable files, libraries). *A priori* this makes sense because it is likely that you will have access to the system's installation media from which applications can be easily installed again on the target computer.

Select Backup Users to include all the files included in all of your users' `/home` directories. Clicking on the Select user manually button lets you select individual users and give you the following options:

- Do not include the browser cache. Selecting this option is recommended due to the very nature of the ever-changing browser cache.

- Use Incremental/Differential Backups. Selecting this will preserve old backups. Choosing Use Incremental Backups will only save files which have been changed or added since the **last** backup operation. Choosing Use Differential Backups will only save files which have been changed or added since the **first** backup operation (also known as the "base" backup). This last option takes more space than the first one, but allows you to restore the system "as it was" at any given point in time for which a differential backup was made.

5.7.1.2. Second Step: Where to Store the Backup
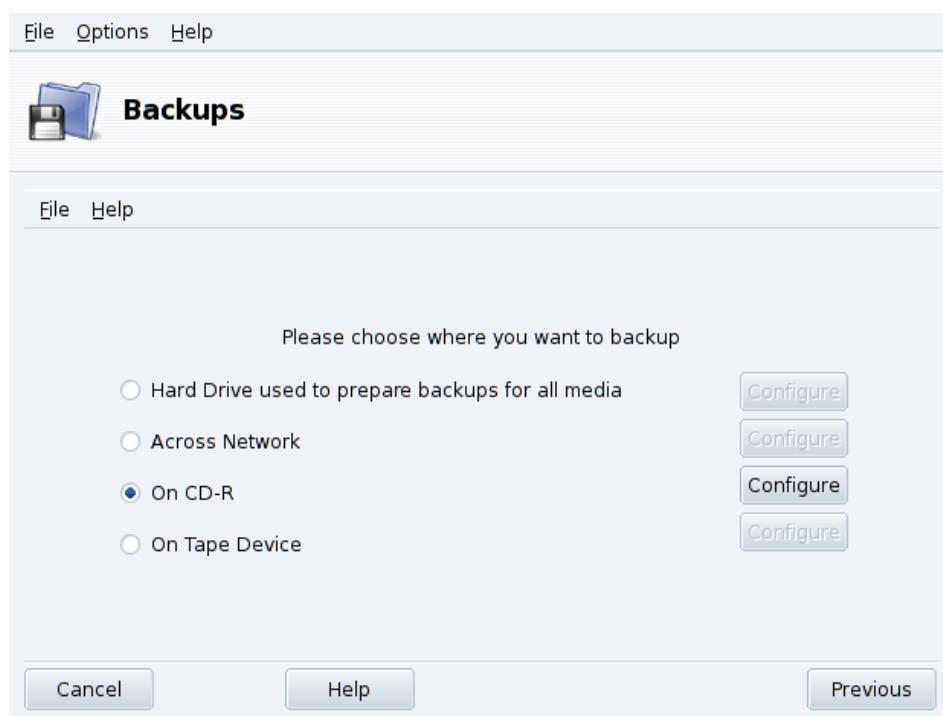
Figure 5-12. Selecting Where to Store the Backup

All possible backup media are listed, along with a Configure button to change media-dependent options:

Hard Disk Drive

The local hard disk drive is used to prepare backups for all media except NFS and direct to tape. You should not perform backups on your local hard disk anyway, you should always backup on remote or removable media. You can set the directory for storage and the limit of storage space. You can also set how many days to keep incremental or differential backups in order to save disk space.

Across the Network

To store the backup on a remote computer accessible using different methods. You can set the connection parameters as well as the access method and its options (if applicable). Please note that NFS backups are considered to be local disk backups, even if they are effectively stored on a remote system.

On Tape

You can set the tape device if it's not detected automatically, and tape parameters such as writing directly on tape, whether or not to rewind, erase and eject the tape.

Optical Media (CD-R)

This is our preferred media for the example, so click on its Configure button to set the required parameters (see figure 5-13).
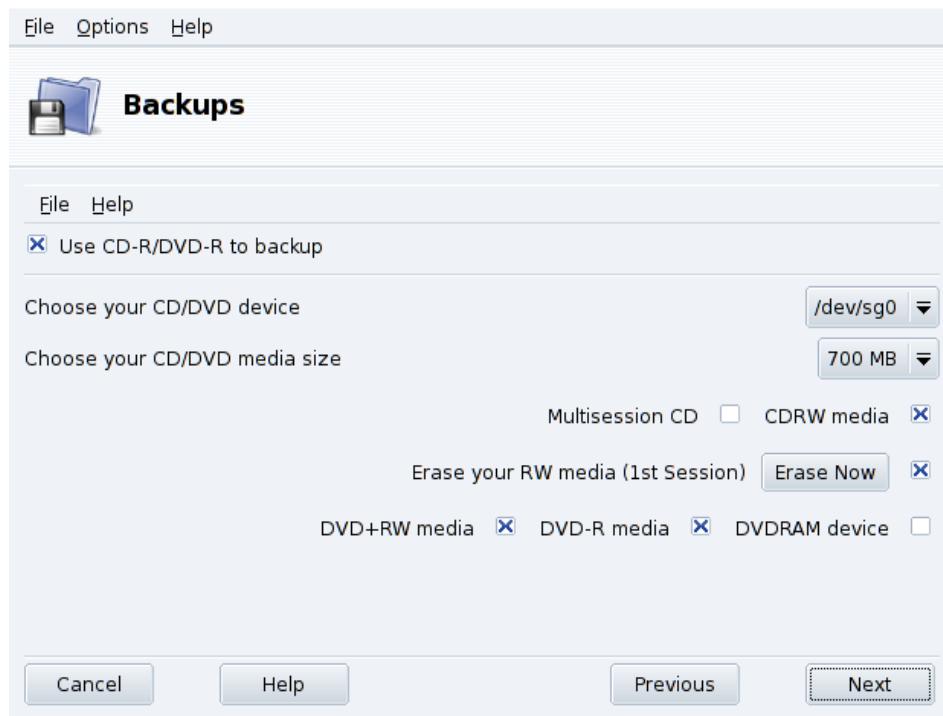
Figure 5-13. Setting Optical Media Parameters

If it isn't done automatically, use the Choose your CD/DVD device combo box to set the CD/DVD device. Set the medium's type and size, multisession and erasing options.

For multisession recordings, please bear in mind that the option to erase the medium is only effective for the 1st session and also that session-related information recording takes some space out (20 to 30 MB) for each session, so the "real data" storage space will actually be less than the medium's size.

5.7.1.3. Third Step: Review and Store the Configuration
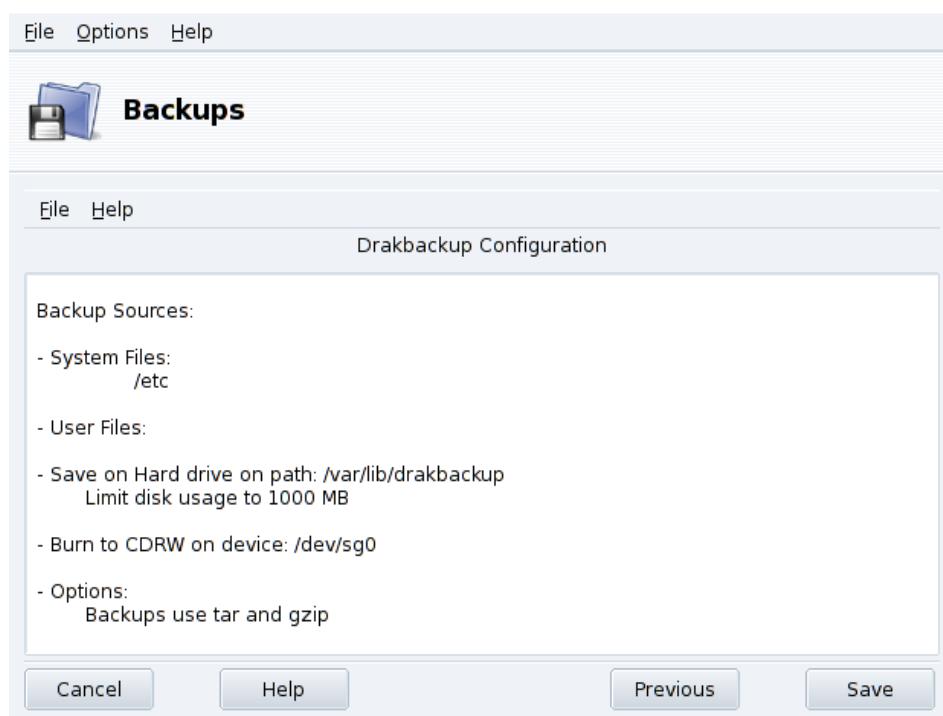
Figure 5-14. Review Configuration Parameters

The last wizard step shows a summary of the configuration parameters. Use the Previous button to change any parameter you are not satisfied with. Click on Save to store them on the `Default` profile. The backup set is now ready to be performed.

Backup Profiles

You can choose File→Save profile as from the menu and provide a profile name to store the current backup settings within a named backup profile. You can then run the configuration wizard again, define other settings and store them under a different profile.

Use the `--profile Profile_Name.conf` option when you run Drakbackup from the command line to load the `Profile_Name.conf` profile.

5.7.1.4. Performing the Backup

Click on Backup Now, make sure the corresponding media is ready (the recordable CDs in our example), and then on Backup Now from configuration file to perform the backup.

Warning

If the backup set size exceeds the medium's available capacity, the backup operation might just fail. This is a known issue and it's being worked on. As a work-around, please try to remove files from the backup set so its size never exceeds the medium's available capacity.

A dialog will display the current progress of the operation. Please be patient: the time it takes to back up depends on many factors such as the size of the backup file set, the speed of the storage option selected, and so on. Once the operation is finished a report is shown: look for possible errors on it and take corrective measures if needed.

5.7.2. Restoring Backups
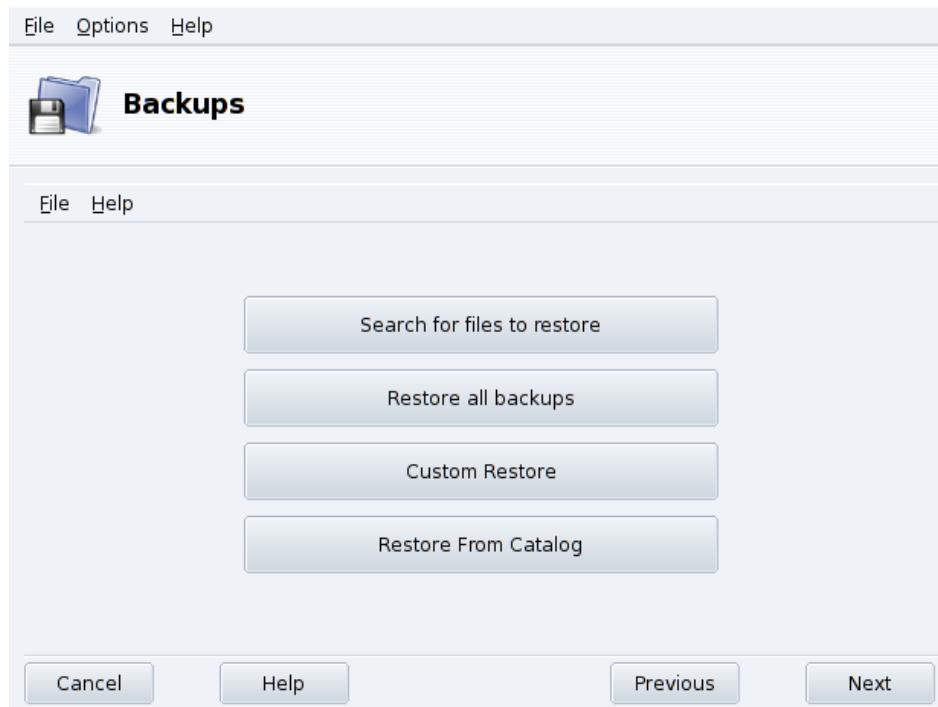
Figure 5-15. Choosing the Restore Type to Perform

Make sure the media you want to restore the backup from is accessible and ready and click on the Restore button. In our example we restore the whole backup so on the restore dialog (figure 5-15) click on Restore all backups and then on the Restore button to start the restoration process.

Warning

Existing files in the target restoration directory (same location where the backup was made from, by default) will be overwritten.
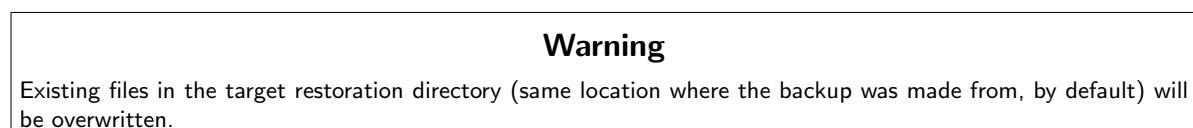
Feel free to investigate the other restore options if you want to restore part of a backup instead of the full file set, or to restore the backup to a different location.

5.7.3. Automating Periodic Backups

In the tool's main window, click on Advanced Configuration and then on the When button. In the backup scheduling window (see figure 5-16) select Use daemon to define the schedule.
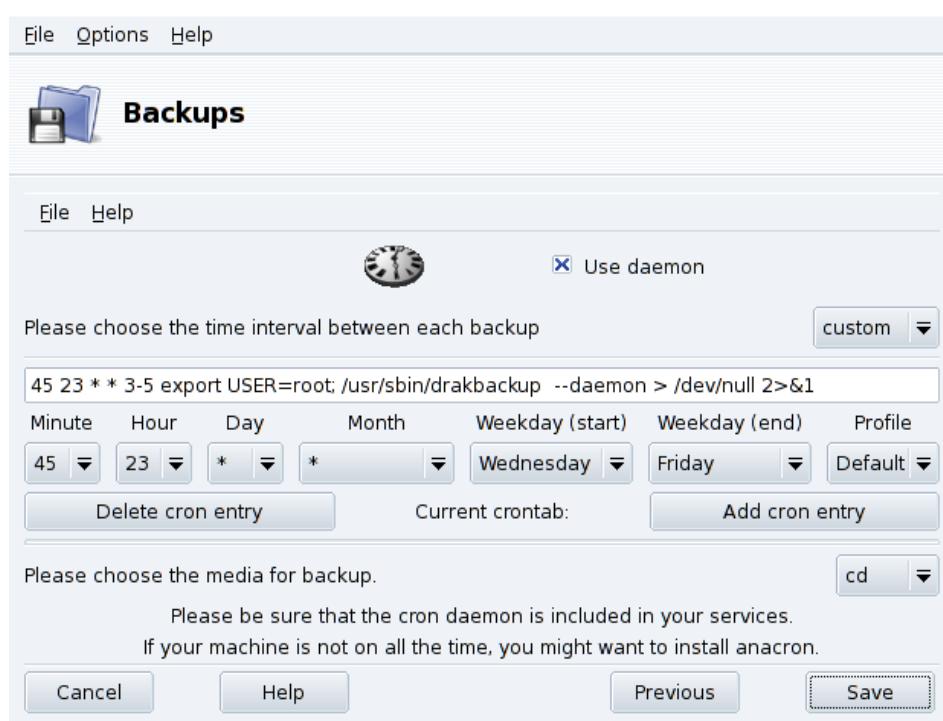
Figure 5-16. Daemon Options Window

You are then asked to specify the interval (or period) between each backup operation and the storage media. In our example we set up a customized calendar (custom period selected) to perform a backup from Wednesday to Friday at a quarter to midnight and store it on CD, using the Default backup profile.

5.7.4. Advanced Backup Wizard Configuration

Click on Advanced Configuration and then on the More Options button to set more backup options (see figure 5-17).
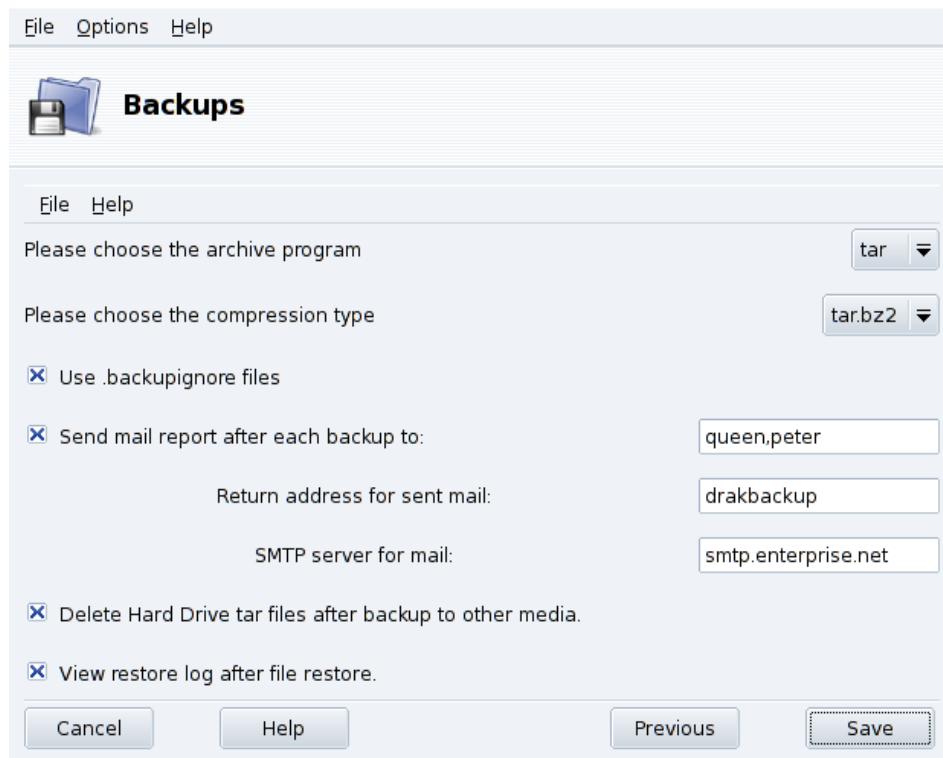
Figure 5-17. Miscellaneous Options Window

Archiving Program

> You can choose between `tar` (the default) and `star` which allows you to backup extended ACLs too.

Compression Type

> You can choose the compression strategy used for your backups among `tar` (no compression), `tar.gz` (`gzip` compression) and `tar.bz2` (`bzip2` compression: better but slower).

Files to Ignore

> You can exclude certain files from the backup. The `.backupignore` file should be present in every directory of the backup file set where files are to be excluded. Its syntax is very simple: a one-file-per-line list of the names of the files to exclude.

> > **Tip:** You can use the star (`*` = "matches any string") and the question mark (`?` = "matches one and only one character, regardless of what that character is") in the `.backupignore` file to exclude sets of files. For example, `somename*` matches all files whose names start with `somename`, and `image00?.jpg` matches files named `image001.jpg`, `image009.jpg`, `image00a.jpg`, `image00h.jpg`, etc.

Send Reports by Email

> Fill the mail address to which a report of the operation will be sent. You can specify many mail addresses separating each with a comma (`,`). Please complete also the Return address for sent mail field with the email address of the backups administrator, and the SMTP server for mail field with the name or IP address of the outgoing mail server.

> > **Tip:** If you want to send the report to more than two or three recipients, it is better if you setup a mailing list, containing all those addresses, and fill the field with the mailing list's post address.

Delete Temporary Files

Select the Delete Hard Drive tar files after backup to other media option to free that space after performing the backup.

View Restore Log

You can choose to view the restore operation log after each restore. This can be handy to spot and fix potential problems when restoring files: reading errors, network communications errors, etc.

Chapter 6. Mount Points and Remote Directories

6.1. Managing your Hard Drive Partitions with DiskDrake

Partitions are initially set up during the installation process. DiskDrake allows you, to some extent, to resize your partitions, move them, etc. DiskDrake can also deal with RAID devices and supports LVM but we will not discuss these advanced uses here.

Warning

DiskDrake is very powerful and can therefore be a dangerous tool. Misuse of it can very easily lead to data loss on your hard drive. Because of this potential loss of data, you are strongly advised to take some protective measures before using DiskDrake:

1. Back up your data. Transfer it to another computer, DVD/CD, etc.

2. Save your current partition table (the table describing the partitions held on your hard drive(s)) to a floppy disk (see *DiskDrake's action buttons*, page 76).

6.1.1. The Interface
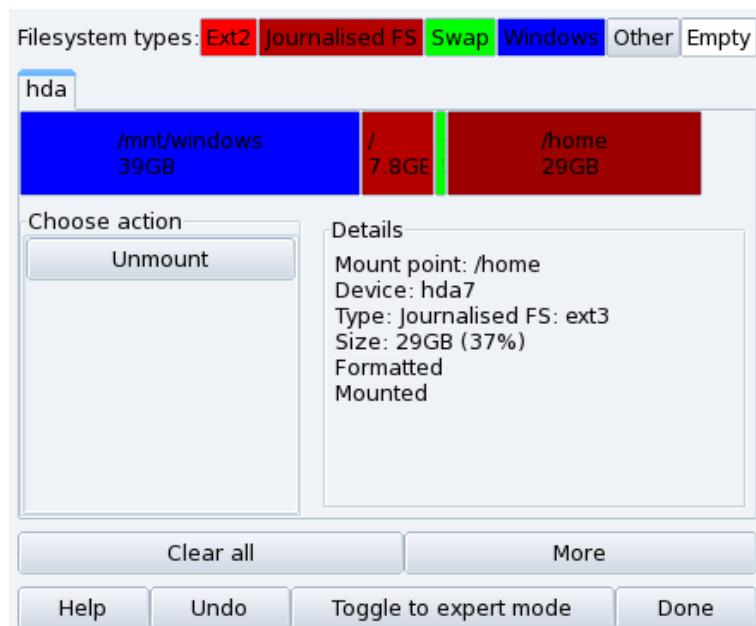
Figure 6-1. DiskDrake's Main Window

DiskDrake enables you to manage partitions on each physical hard drive on your machine. If you only have one IDE disk, you will see a single tab called hda below the file-system types. If there is more than one drive, then each drive will have its own tab and will be named according to the Linux name for that drive.

The window (see figure 6-1) is divided into four zones:

- Top. The structure of your hard drive. When you launch DiskDrake it will display the current structure of the drive. DiskDrake will update the display as you make changes.

- Left. A menu relevant to the partition currently selected in the above diagram.

- Right. A description of the selected partition.

- Bottom. Buttons for executing general actions. See *DiskDrake's action buttons*, page 76.

We will now review the actions available through the buttons at the bottom of the window, and then describe a practical use case.

6.1.2. DiskDrake's action buttons

Clear all

> Clicking on this button will clear all partitions on the current hard drive.

More

> Displays a dialog allowing you to:
>
> **Save partition table.** Allows you to save the current partition table to a file on a disk (a floppy, for example). This may prove useful if a problem arises (such as an error made during drive repartitioning).
>
> **Restore partition table.** Allows you to restore the partition table as previously saved with Save partition table. Restoring a partition table may recover your data as long as you do not reformat partitions, because the formatting process overwrites all your data.
>
> **Rescue partition table.** If you lose your partition table and have no backup, this function scans your hard drive to try and reconstruct the partition table.

Help

> Display this documentation in a browser window.

Undo

> Cancels last action. Most modifications done on your partitions are not made permanent until DiskDrake warns you it will write the partition table. This button therefore allows you to undo all of your modifications on partitions up to last write.

Toggle to expert mode

> This button allows you to access the expert mode functions (which are even **more** dangerous if you are not sure what you are doing). Reserved for experts.

Done

> Saves your changes and exits DiskDrake.

## 6.1.3. Resizing an Old Partition and Creating a New One

In this section, we are going to do a little exercise to demonstrate one of the more useful features of DiskDrake. Let us imagine that you decide to use your machine as an FTP server and you want to create a separate `/var/ftp` partition in order to host the FTP files. **Note that doing this step-by-step tutorial will actually modify the structure of your hard drive.**

1. Reboot the machine and choose Menu→Console Login at the login screen.
2. Login yourself as `root` and run command **`xinit diskdrake`**
3. This is what the current `/home` partition looks like before any modification. We are going to shrink this partition in order to create free space for the new file system.
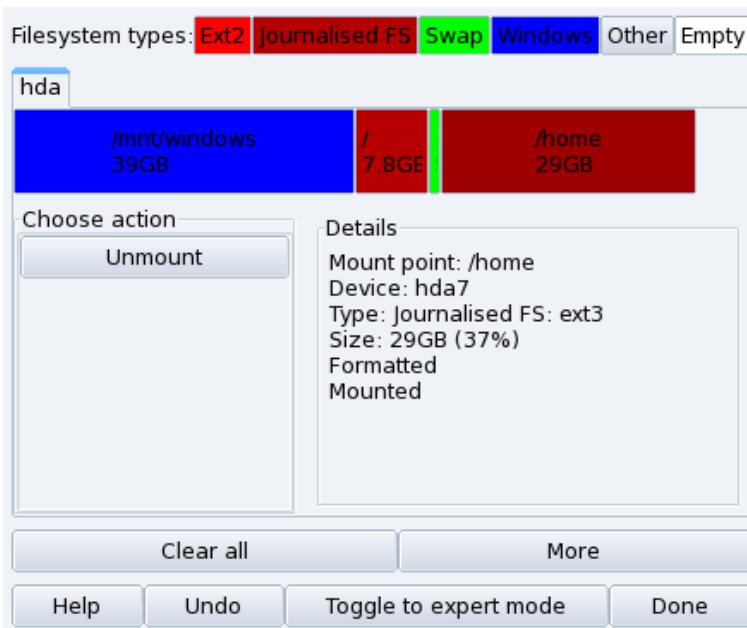
First of all, you need to unmount the `/home` partition by clicking on it and then pressing the Unmount button.

4. The next step, as you may have guessed, is to click on the Resize button. A dialog appears which allows you to choose the new size for the `/home` partition. Move the slider to reflect the new size, then click on OK.

5. When this is done, you will notice that the graphic representation of your hard drive has changed. The `/home` partition is smaller, and an empty space appears on the right. Click on the empty space and then on the Create button which appears. A dialog will let you choose the parameters for the new partition. Set the size, choose the file system you want to use (usually `Journalized FS: ext3`) and then enter the mount point for the partition, which in our example will be `/var/ftp`.

This is how our projected partition table now looks like.

6. The last step is to format (prepare to host files) the newly created partition. To format the partition, click on its representation in the partitions picture, then on the Format button. Confirm the writing of the partition table to disk, the formatting of the partition and the update to the `/etc/fstab` file. You may be asked to reboot the computer to make changes effective.

6.2. Managing Removable Devices

 These tools enable system administrators to easily control those options which affect the behavior of removable devices such as floppy, CD and DVD disks. Note that, by default, all removable devices are automatically made available so users shouldn't need to manually mount media.

Figure 6-2. Changing a Parameter

For each device the following properties may be changed:

- **Mount point.** The directory from where the device's files will be accessed. You can either choose an entry from the list or type in your own path. If the directory does not exist, it is created automatically.

- **Options.** Controls various device options, notably whether a user is allowed to use new media without root privileges. If the user option (available by clicking the Advanced button) is deselected, regular users won't be able to access newly inserted media on this drive, only root will be able to access it.

- **Type.** Displays a list of file-system types. If you have a specific medium with a different file system on it, this is where you can tell Linux how to access it.

Select the property you wish to change and click OK. The corresponding dialog pops up in which you can change your settings. Then click OK again. The system then asks you if you want to save the modifications in the `/etc/fstab` file. By saying yes, you will not have to unmount and re-mount that device: it is done automatically

6.3. Importing Remote SMB Directories

This tool allows the system administrator to give users access to remotely shared directories using the SMB protocol (used mainly by Windows®).

While users can individually access remote shares through their file managers, it may be required in some cases to import a specific share for it to become immediately available for all users. We'll go through an example showing you how to import a directory from a Windows® machine.
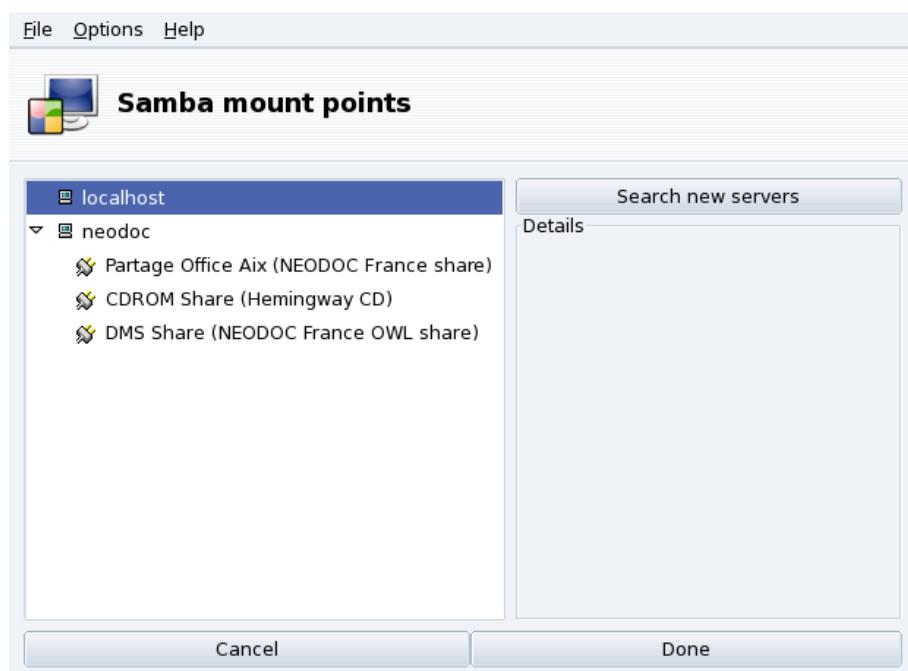

Figure 6-3. Scanning the Whole Network

Choose a Server. Clicking on the Search servers button scans the local network for machines which currently share directories (including the local one). We'll choose one of them and make it available locally for all users.

Choose a Share. Clicking on a machine's name will try to connect to it and browse for available shares. If that machine has password-protected shares, a dialog pops up asking you to identify yourself. Enter the correct Username, Password and Domain. The available shares on that machine will then appear. Click on the little arrow at the left of the machine icon to show available shares.

> **Tip:** If the machine you're connecting to has both public and password-protected shares, then canceling the password entry dialog will connect you to that machine, but only to its public shares.

Figure 6-4. Choosing the Remote Directory to Import

Once a share is selected, a Mount point button appears. Clicking on it displays a dialog where you can type the local directory name where remote files will be accessible.

Once this is done, two more buttons appear:

- **Mount.** Makes the resource available locally. When this is done, users simply have to point their file manager to the directory selected as the mount point to get the files hosted by the server.

- **Options.** Allows you to set a user name and password to access that SMB mount point. Other permissions and advanced settings can also be set through this button.

Import Share on Each Reboot. When you're finished configuring the access points for remote directories, click on Done. A dialog box will appear asking you whether you wish to save your modifications to the `/etc/fstab` file (where mount point information is usually stored), or not. Click on Yes to make the shares configuration persistent between sessions. Click on No to exit without saving your changes.

6.4. Importing Remote NFS Directories

This tool is exactly the same as the one mentioned in *Importing Remote SMB Directories*, page 79, except that it controls file sharing through the NFS protocol rather than SMB. Therefore it allows you to locally import shared files from NFS-friendly machines. The interface is the same as the one described in *Importing Remote SMB Directories*, page 79, and the effects are similar. Only the corresponding machines are different: UNIX® for NFS and Windows® for SMB.

One other difference is that there is no need to provide a password to access NFS shares. The authentication mechanism is host-based.

6.5. Allowing Users to Share Folders
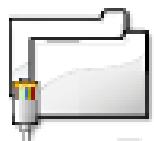
This tool enables you to share files with other users of your computer network. File sharing can be done on heterogeneous systems such as GNU/Linux and Windows®.

The file-sharing configuration is done in two simple steps: determining who can export folders, and then which protocol to use. A third step is necessary if you select the Custom export option.

Figure 6-5. Controlling Exports

1. Who is Allowed to Share Folders

   - **No sharing.** Prevents users from sharing data with others.

   - **Allow all users.** All users are allowed to share data with others.

   - **Custom.** By choosing this option, only users within the same `fileshare` group will be allowed to share data. If you choose this option, the `fileshare` group will be created and, as a 3rd step, you will be prompted to run UserDrake in order to add the allowed users to this group (see *Managing Users and Groups*, page 63).

2. Choose the Export Protocol

   You must now choose which protocol to use for file sharing. Check one or both of the following:

- **SMB.** If most of your users use Windows® systems, this is the preferable protocol to select.
- **NFS.** If most of your users use UNIX® systems (such as GNU/Linux), this is the preferable protocol to select.

3. Once you have checked the appropriate boxes, click on OK. The required packages will be installed, if needed. If you uncheck a previously checked box, the corresponding service will be stopped.

Users Can Now Share Folders. Once users are allowed to share data, they can select the folders to be shared through their preferred file manager.

6.6. Setting up WebDAV Mount Points

WebDAV (*Web-based Distributed Authoring and Versioning*) is an extension to the HTTP protocol which allows you to create, move, copy, and delete resources on a remote web server. In practice, mounting a remote WebDAV repository on your local machine allows users to modify a remote web server's files as if those files were local to the system.

Tip: Browse the WebDAV Resources (`http://www.webdav.org/`) pages to learn more about this protocol.
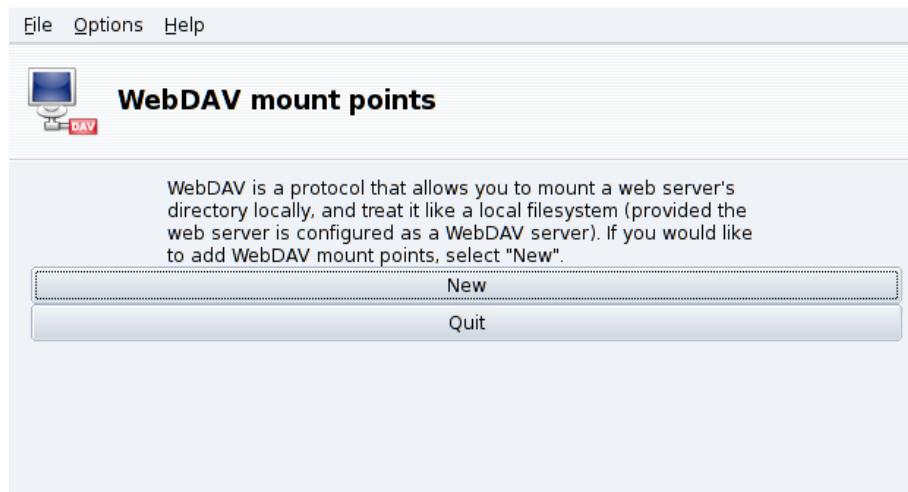
Figure 6-6. Managing WebDAV Mounts Points

The first time you launch this tool the required packages are installed if needed, and only two buttons are available. New, which allows you to define a new mount point, the other one just Quits the application. After you have defined mount points, they will appear as new buttons at the top of the buttons list. Clicking on a mount point button will take you to the mount point menu (see figure 6-7).

When you click on the New button you are asked for the URL of the web server. Enter the complete URL of the web server, beginning with `http://` or `https://`, then click OK.
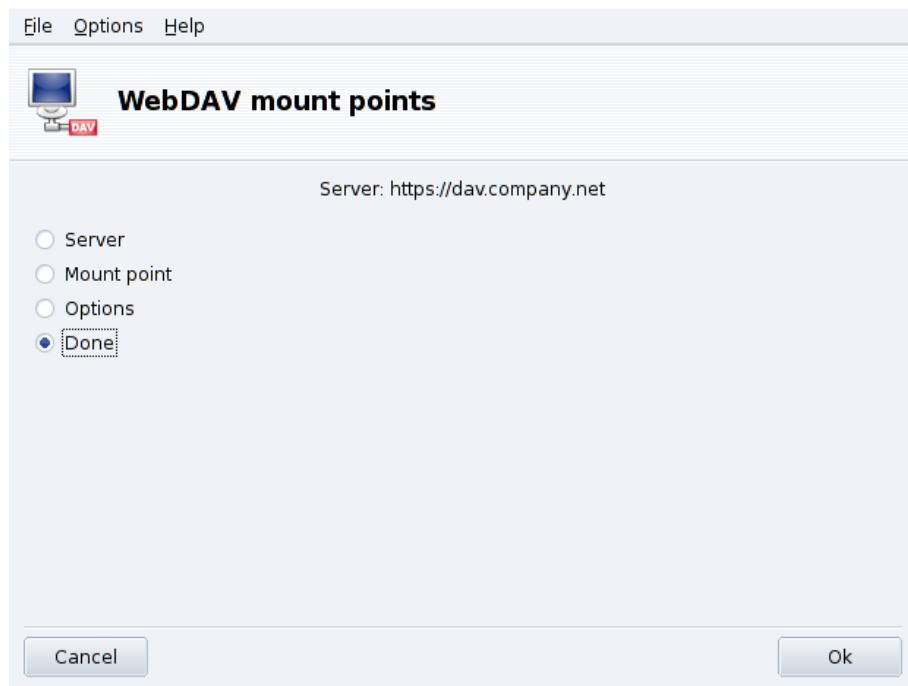
Figure 6-7. WebDAV Menu

You must now decide where the web server files will be accessible from. Select the Mount point option and click OK. There you are able to choose a local directory or type in your own. If the selected mount point does not exist, it is created.

If the server requires authentication, do not forget to fill the username and password fields in the Options dialog. Then all you need to do is to actually mount the remote repository by selecting Mount and clicking OK.

You are now able to browse and modify files on the local mount point you have defined and the changes will be immediately available on the web server.

To make your settings persistent between sessions, remember to save modifications to the `/etc/fstab` file, as suggested when you quit the wizard.

Chapter 7. "Security" Section

7.1. Securing your Machine through DrakSec

draksec is a graphical interface to msec (which stands for Mandriva Linux Security Tool). It allows you to change your system's security level and to configure every option of msec's security features.

msec has two aspects: system behavior configuration and periodic checks of system state. Each security level modifies the system configuration, making it more and more secure, and verifying more and more security related aspects.

7.1.1. Setting your Security Level

> **Expert Tool:** This tool is only displayed in expert mode. Choose Options→Expert mode from the menu and then access the Security section of Mandriva Linux Control Center.
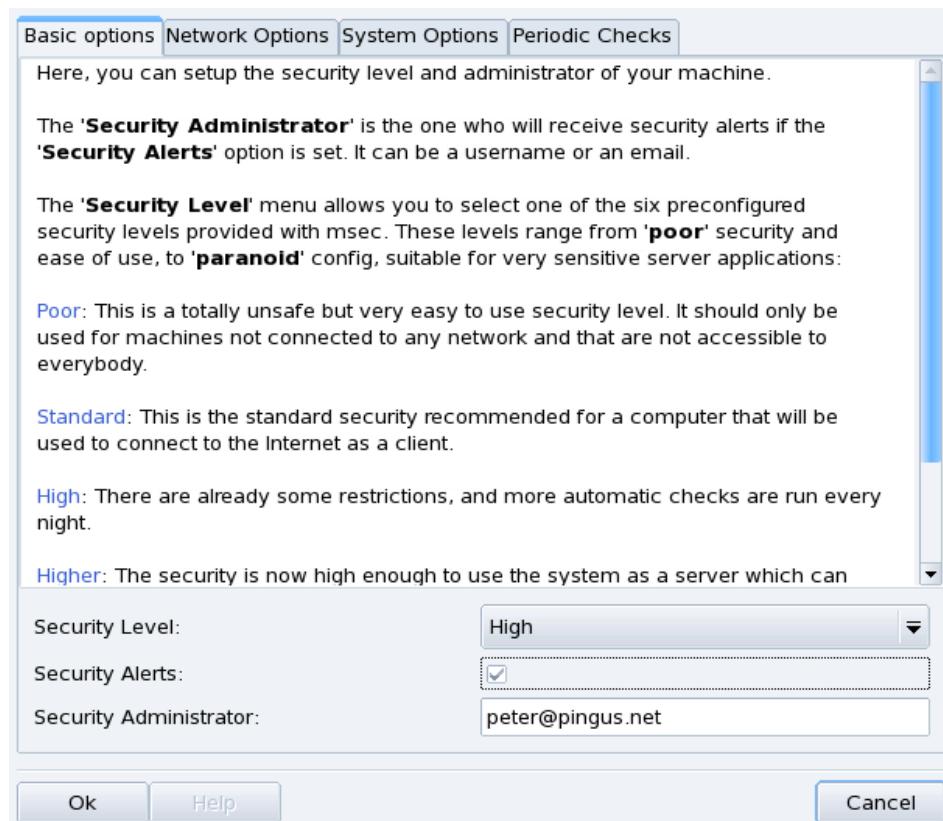
Figure 7-1. Choosing the Security Level of your System

Choose a Security Level. Simply choose the security level you want from the Security Level pull-down list: it will be effective as soon as you click on OK. Please read the help text regarding security levels very carefully so that you know what setting a specific security level implies.

> **Explore Each Level:** If you wish to check which options are activated for each security level, review the other tabs: Network Options, System Options and Periodic Checks. Click on the Help button to display information about the options and their default values. If some of the default options don't suit your needs, simply redefine them. See *Customizing a Security Level*, page 86, for details.

Activate Security Alerts. Put a check mark on the Security Alerts box to send by mail possible security issues found by msec to the local user name or to the e-mail address defined in the Security Administrator field.

Warning
We highly recommend you activate the security alerts option so that the administrator is immediately informed of possible security issues. Otherwise the administrator will have to regularly check the relevant system log files.
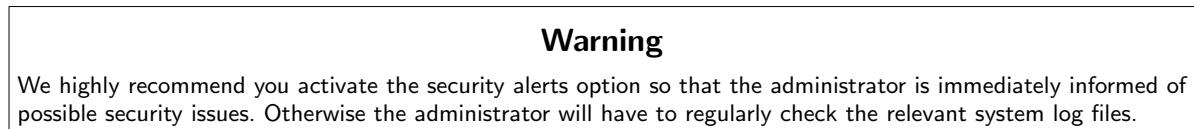
7.1.2. Customizing a Security Level

Clicking on each of the Options tabs (and the Periodic Checks one) lead you to msec's list of security options. This allows you to define your own security level based on the security level previously chosen.
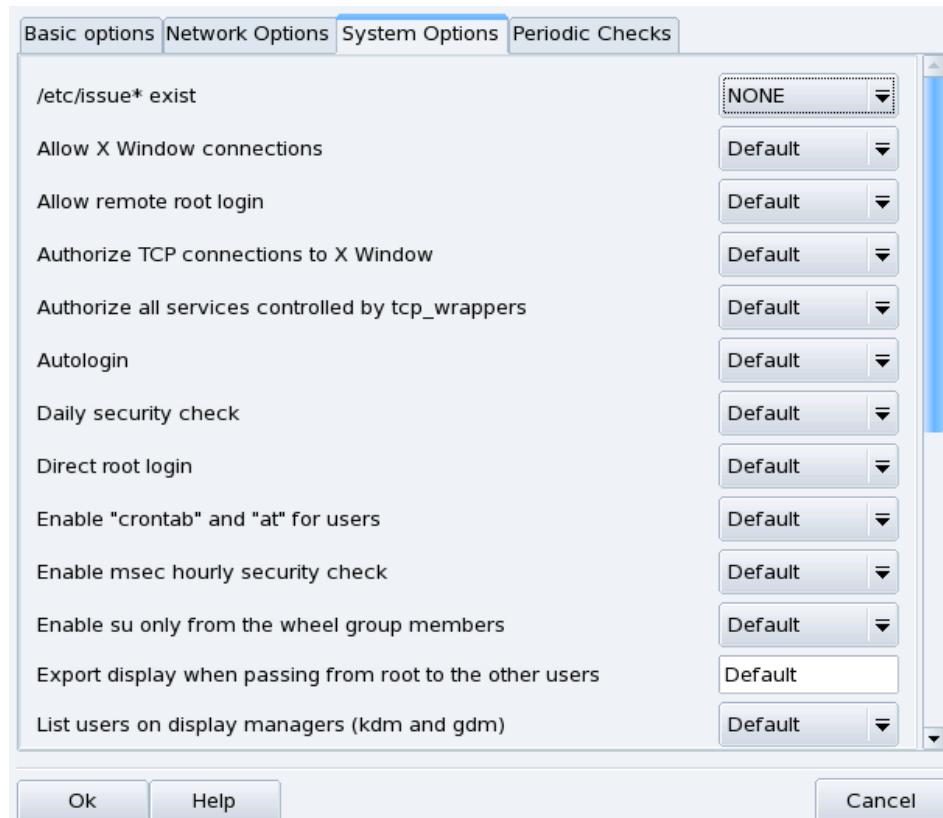
Figure 7-2. Modifying Standard Options

For each tab, there are two columns:

1. **Options List.** All available options are listed.
2. **Value.** For each option[1] you can choose from the corresponding pull-down menu:
   - **Yes.** Activate this option no matter what the default value is.
   - **No.** Deactivate this option no matter what the default value is.
   - **Default.** Keep the default security level behavior.
   - **Ignore.** Use this value if you don't wish this test to be performed.
   - **ALL, LOCAL, NONE.** The meaning of these are option-dependent. Please see the Help text available through the Help button for more information.

Clicking on OK accepts the current security level with custom options, applies it to the system and exits the application.

---

1. The default security level setting is shown in the Help window.

7.2. Controlling File Permissions with DrakPerm

drakperm allows you to customize the permissions which should be associated with each file and directory in your system: configuration files, personal files, applications, etc. If the owners and permissions listed here don't match the actual permissions of the system's files, then msec (which stands for *Mandriva Linux Security Tool*) will change them during its hourly checks. These modifications can help prevent possible security holes or intrusions.

Note: This tool is accessible only in expert mode. Choose Options→Expert mode from the menu and then access the Security section of Mandriva Linux Control Center.
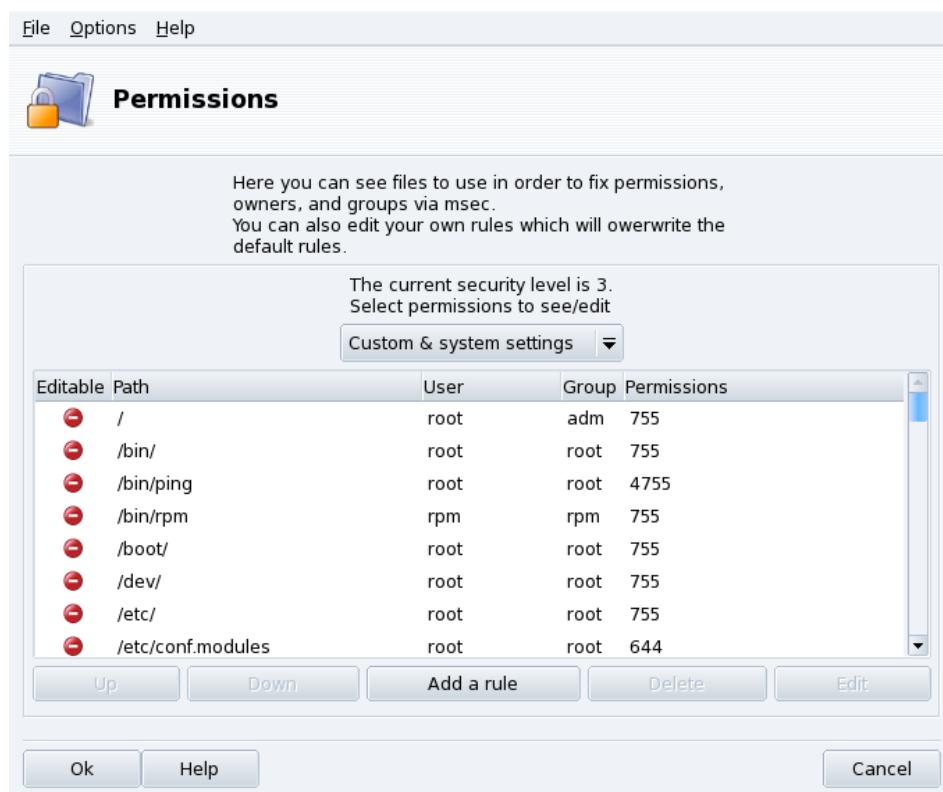
Figure 7-3. Configuring File-Permission Checks

The list of files and directories which appears depends on the current system's security level as set by msec, along with their expected permissions for that security level. For each entry (Path) exists a corresponding owner (User), owner group (Group) and Permissions. In the drop-down menu, you can choose to display only msec rules (System settings), your own user-defined rules (Custom settings) or both as in the example shown in figure 7-3.

Note: You cannot edit system rules, as stated by the "Do not enter" sign on the left. However you can override them by adding custom rules.

Create Your Own Rules. If you wish to add your own rules for specific files or modify the default behavior, display the Custom settings list and click on the Add a rule button.
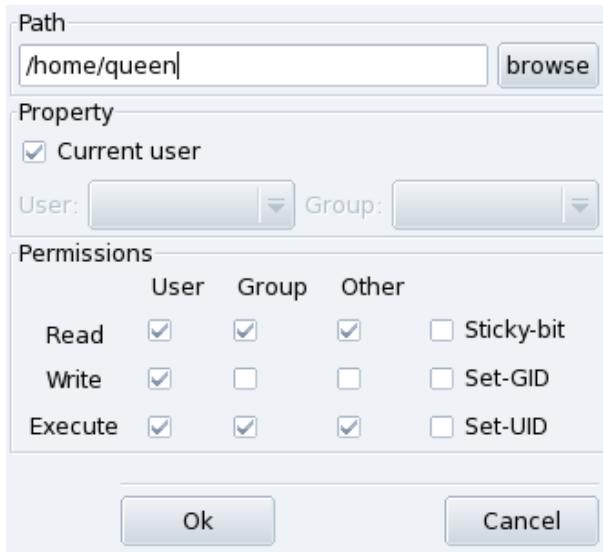
Figure 7-4. Adding a File-Permissions Rule

Customize Your Home Directory Permissions

1. Create a New Rule in msec

   Let's imagine your current security level is set to 3 (high). This means that only the owners of the home directories can browse them. If you wish to share the content of Queen's home directory with other users, you need to modify the permissions of the `/home/queen/` directory.

2. Actually change the Home Permissions

   msec only changes file permissions that are more permissive than the one required by a certain security level. That means that for the change above, the permissions must be changed by hand.

   You can do this in Konqueror by modifying the permission properties of your home directory, and checking the Apply changes to all sub-folders and their contents option.

3. Check Rules Priority

   If you create more rules, you can change their priorities by moving them up and down the rules list: use the Up and Down buttons on your custom rules to have more control over your system's permissions.

7.3. Securing your Internet Access via DrakFirewall

 This little tool allows you to set up a basic firewall on your machine. It filters connection attempts made from the outside, and blocks unauthorized ones. It's a good idea to run it just after installing your machine and before connecting to the Internet, therefore minimizing the risks of your machine being ccompromised.

This Wizard consists of the three steps we detail below.

7.3.1. Choose Services to be Available from Outside
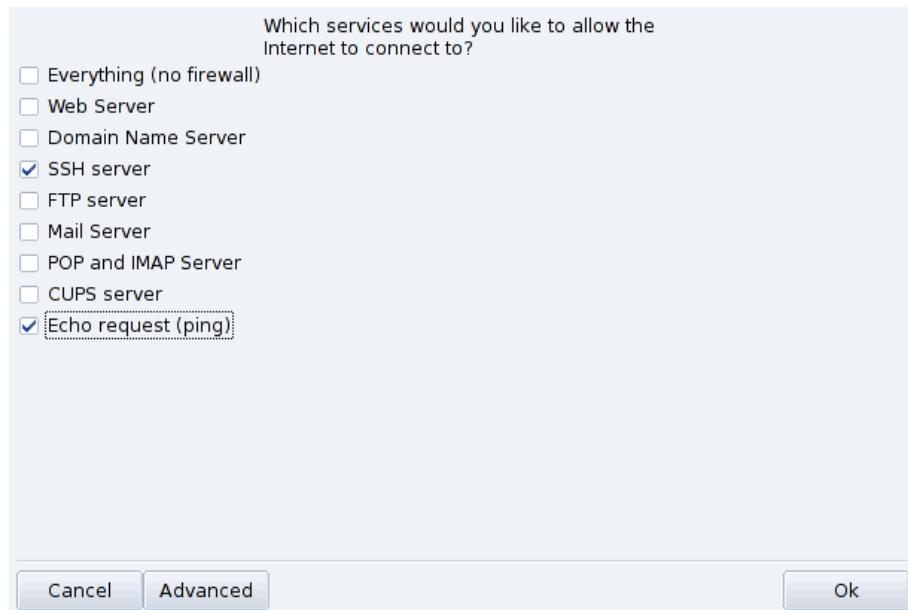
Figure 7-5. The DrakFirewall Window

Open Up Ports, If Needed. If checked, uncheck the Everything (no firewall) box, and then check the boxes corresponding to the services you wish to make available to the outside world. If you wish to authorize a service which isn't listed here, click on Advanced to manually enter the port numbers to open.

> **Opening Unusual Services:** The Advanced button opens a field named Other ports where you can enter any port to be opened to the outside world. Examples of port specifications are presented just above the input field: use them as a guide. It's possible to specify port ranges by using the `:` syntax such as `24300:24350/udp`.

This Won't Block You from Accessing the Net. Not checking a service in this list won't stop you from connecting **to** it. It will only prevent people **from** the Internet connecting to that service on your machine. If you don't plan on hosting any services on your machine (common case for a desktop machine) just leave all boxes unchecked.

How to Disable the Firewall. On the other hand if you wish to disable the firewall and leave all services accessible from the outside, check Everything (no firewall), but please bear in mind that this is **very insecure**, and therefore not recommended.

7.3.2. Activate Interactive Firewall Feature

Figure 7-6. Interactive Firewall Options

Stay Informed of Connections on your Machine.

The interactive firewall can warn you of connection attempts on your machine by displaying alert popups through the network applet. Check the Use Interactive Firewall option to activate this feature.

Port scan detection

Activate this option to be warned of malicious attempts to access your machine.

Other entries corresponding to open ports

Next you are shown a checkbox for each port you have chosen to open during the previous step. Activating them will popup a warning each time a connection attempt is made on those ports.

7.3.3. Which Interface to Protect

The next step consists of selecting the network interface connected to the Internet.

Please select the interfaces that will be protected by the firewall.

All interfaces directly connected to Internet should be selected,
while interfaces connected to a local network may be unselected.

Which interfaces should be protected?

☐ Ethernet: eth0
☑ WiFi: eth1

Ok
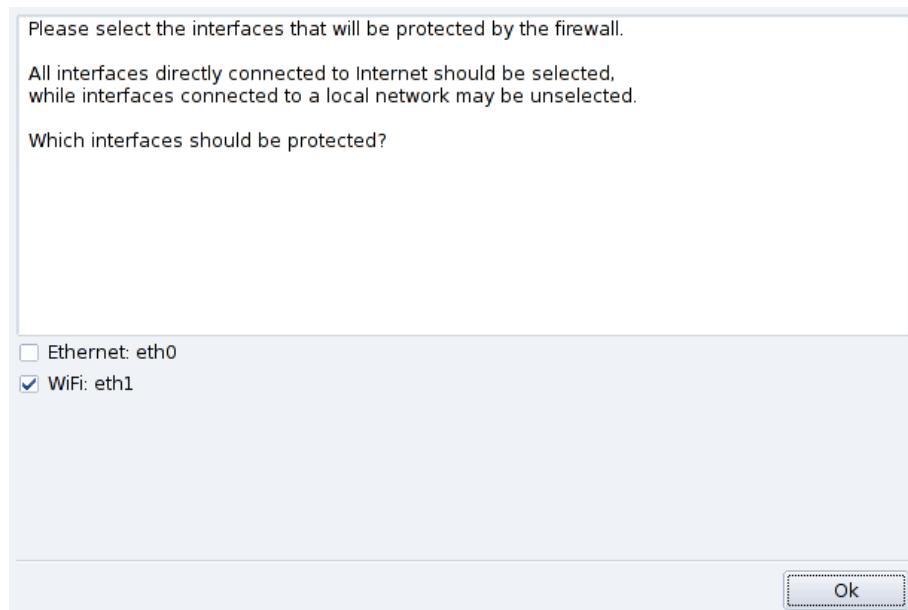
Figure 7-7. The Internet Interface

If you don't know which interfaces you have connected for the Internet, you can check the system network configuration (see *Reconfigure Interfaces*, page 48). You can finally click OK to install the required packages, activate the firewall and enjoy your secure Internet connection.

Chapter 8. "Boot" Section

8.1. Configuring the Login Mode

This tool allows a user to be automatically logged into the system at boot time, without a password being required.
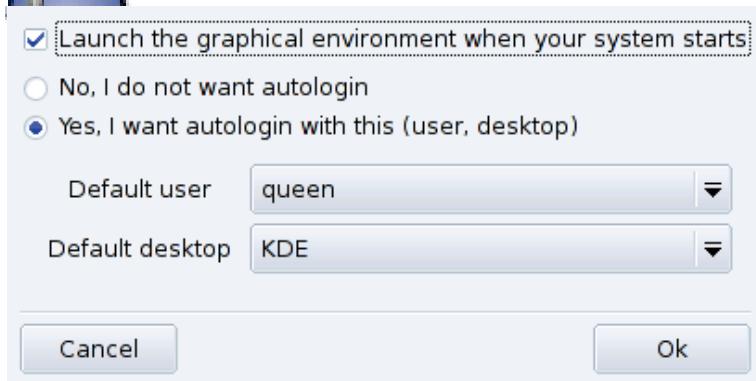
Figure 8-1. Choosing the Login Mode

Here are the available parameters:

Graphical Interface

If you wish to have the X Window System (graphical display) started at boot time, check the Launch the graphical environment when your system starts box. If you leave it unchecked, the text login will be displayed and you will need to start the graphical environment manually.

Autologin

If you're the only person using your machine and nobody else has access to it, you may choose to be automatically logged in at boot time.

1. Select the Yes, I want to autologin with this (user, desktop) option.

2. Choose the user you want to be logged on automatically in the Default user pull-down menu.

3. Choose the preferred Default desktop in the pull-down menu.

8.2. Changing your Boot-up Configuration

This tool allows you to configure the bootloader and the boot menu entries.

Warning

Unless you're an expert, it's not recommended that you change these settings as this may prevent you from booting your machine the next time you try to power it on.
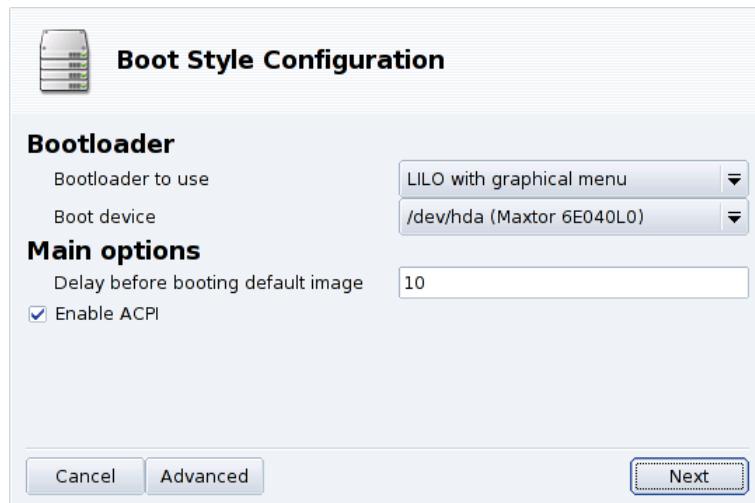
Figure 8-2. Choosing the Boot Mode

8.2.1. Configuring the Bootloader

You can choose between the GRUB and the LILO bootloader. Either one will allow you to boot Mandriva Linux, it's just a question of taste.

Unless you know what you're doing, you shouldn't change the default Boot device shown, since that's where the bootloader installs itself. If more than one OS is installed on your machine, it's a good idea to leave at least 5 seconds so that you can easily select a different menu item than the default image.

The dialog finally shows a few options which can be useful depending on your specific hardware.

Enable ACPI

> Enable this option to allow better power management support if your hardware is ACPI compatible. ACPI is often needed for new laptops which no longer support APM.

Advanced options. Click on Advanced to be able to wipe the contents of the /tmp directory (which might hold some files you download from the Internet, for instance) and to tell Linux how much RAM your machine has, should this prove to be an issue at boot time.

8.2.2. Managing Boot Entries

After clicking Next, the list of available entries at boot time is displayed; the default one is marked by a star (⋆).

It's also possible to make an entry the default one by checking the Default check-box in the Modify dialog.

8.3. Customizing your Boot Theme

The Boot Theme utility enables you to change the default theme displayed at boot time, as well as a few other options.

- Choose one of the available boot modes in the pull-down menu (figure 8-3).
- Uncheck the Display theme under console option if you want a clean, "traditional" console. This relates to those accessible through the **Ctrl-Alt-Fn** keys.
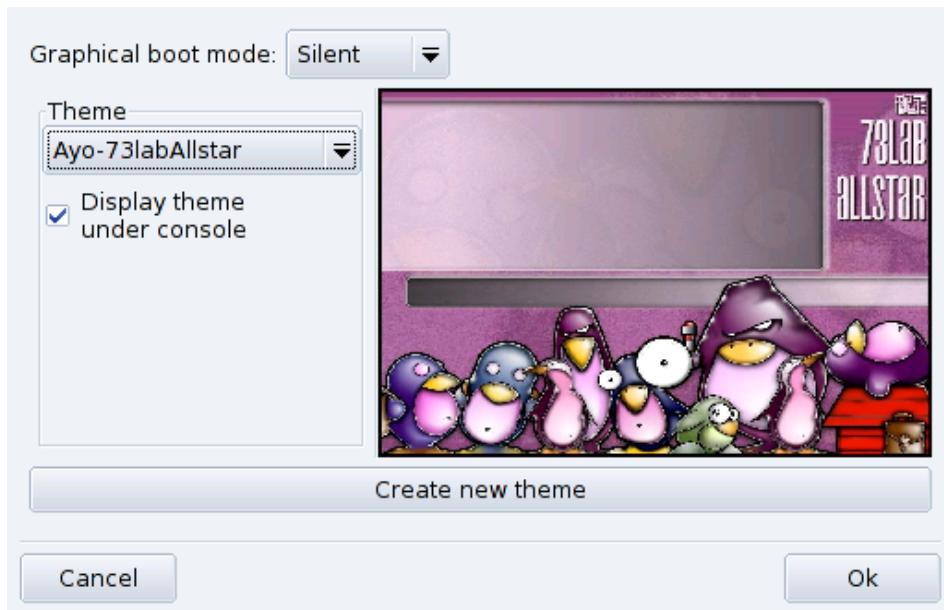
Figure 8-3. DrakBoot Theme Window

The boot theme setting will have no effect if your system isn't set to boot using the graphical mode. Please refer to *Changing your Boot-up Configuration*, page 93, for more information on setting the boot mode.

Installing Fancy New Themes. If you only have one theme available, you may install the `bootsplash-themes` package which you will find in `contribs`. Other themes are also available on the web.

Create Your Own. The Create new theme button allows you to fully customize an existing boot theme or create a new boot theme from scratch. Adjust the parameters to your liking and save it. It will then be accessible in the available Themes list.

Chapter 9. Server Configuration Wizards

9.1. Foreword

The Mandriva Linux configuration wizards are designed to configure servers located between a local network and the Internet. They let you quickly and efficiently configure the most common services in a local network, as well as Internet web and FTP services. We assume that your network is as shown in figure 9-1, and that Mandriva Linux is installed on the server. Configuring and bringing up the Internet connection is beyond the scope of this chapter (see *Network and Internet Connection Management*, page 43).
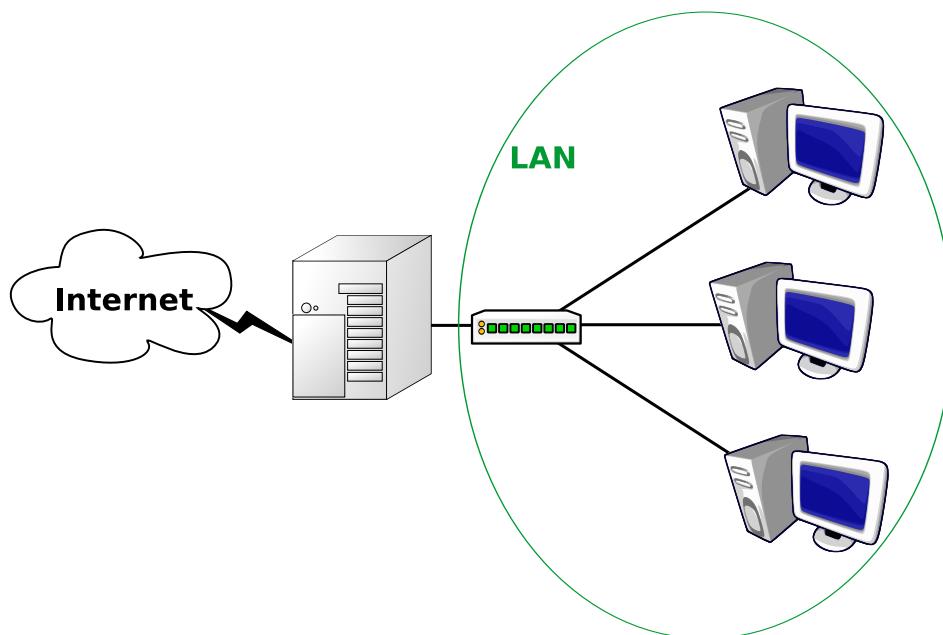
Figure 9-1. An Example of an Internal Network

The server configuration wizards are available through the Control Center when the `drakwizard` package is installed. New categories appear in the Mandriva Linux Control Center, so wizards are organized as follows:

> **Note:** Wizards noted as "Expert mode only" below are only accessible when the expert mode is toggled on (Options→ Expert mode).

Sharing

- FTP server (*FTP Server Configuration*, page 105): configure where your FTP server should be reachable from.

- Samba server (*Samba Server Configuration*, page 102): this wizard helps you set up public shared files and printers, and announce their names to the Windows® network.

- Samba server fine tuning: this set of wizards let you manage and create shares for repositories (public/user shares). Expert mode only.

- Web server (*Web Server Configuration*, page 104): to setup your GNU/Linux box as a web server. We explain how to make it reachable from the Internet.

- Installation server (*Installation Server Wizard*, page 108): to allow your network client machines to be installed from the server, making CDs and DVDs obsolete. Expert mode only.

Network Services

- DHCP server (*DHCP Server Configuration*, page 98): your server can assign IP addresses dynamically to machines on the network.

- DNS server (*DNS Server Configuration*, page 99): to configure name resolution for machines inside and outside the private network.

- Proxy server (*Proxy Server Configuration*, page 110): configure your server to act as a web proxy cache. This speeds up web browsing while limiting the bandwidth usage on the Internet.

- Time server (*Time Configuration*, page 112): your machine can also supply time to other machines using NTP (*Network Time Protocol*).

- OpenSSH server: to let people connect to your server, and use its console "as if they were sitting there", through a secure communications channel.

Authentication

- Change authentication method: to set up the local users authentication scheme (local, LDAP, NIS, Windows Domain). Expert mode only.

- NIS server (*NIS and Autofs Servers Wizard*, page 108): to set up the Network Information System, centralizing users authentication and home directories.

- LDAP server (*LDAP Configuration Wizard*, page 109): to set up a simple LDAP repository to be used as authentication mechanism.

Groupware

- Mail server (*Mail Server Configuration*, page 100): configure your mail domain for sending and receiving mail to and from the outside world.

You can access the wizards by clicking on their corresponding buttons. We describe wizards for the most common services in no particular order. Note that the required packages are installed by the wizard if they are not already available.

Note: For experienced users: wizards are limited to configuring class C networks, and only the basic configuration is handled for each service. This should be enough for most situations, but if you wish for a more fine-tuned configuration, you must edit the configuration files by hand or by using another administration tool such as Webmin.

9.2. DHCP Server Configuration

DHCP stands for *Dynamic Host Configuration Protocol*. This protocol allows for machines connecting to your local network to be automatically assigned all relevant network parameters such as an IP address, the addresses of the name servers and the address of the gateway.
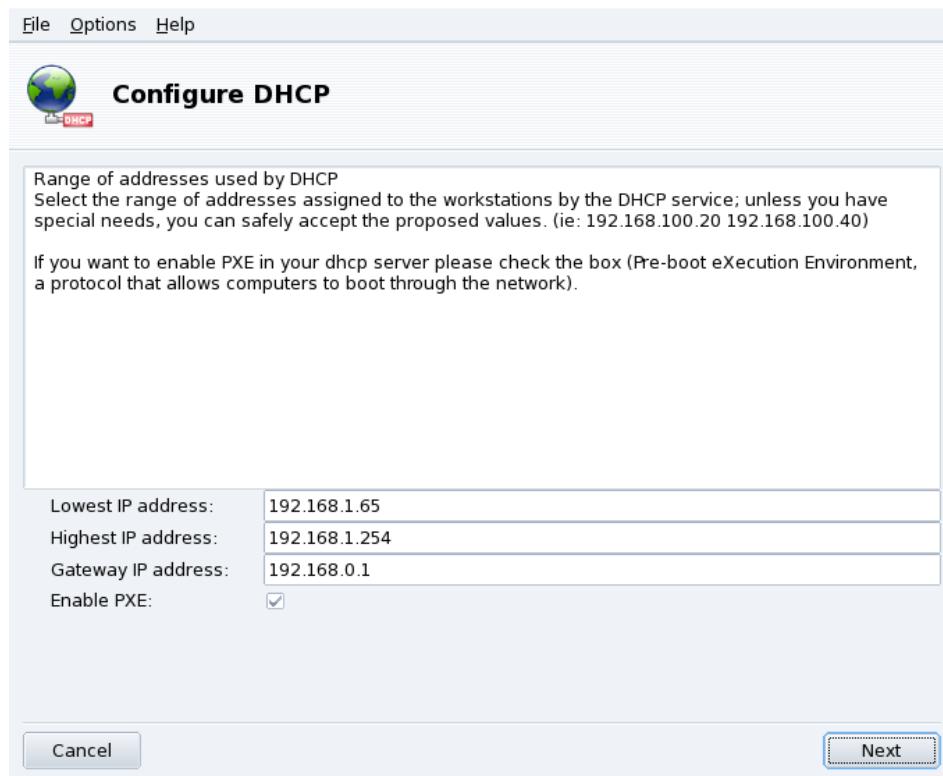
Figure 9-2. DHCP Server Address Range

All you have to do is specify the range of addresses[1] that you want to have available via DHCP, as shown in figure 9-2. Select the network interface the DHCP server must listen on for requests: choose the one connected to your LAN. If you wish that client computers be able to access the Internet, you need to provide the IP address of the gateway. In case the DHCP server is also the gateway for your LAN fill it with the server's LAN address (for example: `192.168.0.1`).

> **Tip:** Check the Enable PXE option if you want your machine to act as an installation server for multiple machines on your LAN.

9.3. DNS Server Configuration

 DNS stands for "Domain Name System". It allows you to specify a machine by its name instead of its IP address. This wizard allows you to setup a basic DNS server, master or slave.

Make sure you have a FQDN host name set for your system, otherwise the DNS wizard will refuse to start. Please refer to *Network and Internet Connection Management*, page 43, for information on how to set the system's host name. You are given the option to run one of the following wizards:

Master DNS Server

Setup your machine as a plain DNS server. After selecting the network interface on which to listen for DNS requests, you can provide the address of an external DNS server to which the requests that the local server cannot answer will be forwarded. It is generally the address of your ISP's DNS server.

Then you can specify domain names for lookups. For example if you request the IP of a machine called `kenobi`, the server appends the domain names you add here to perform the request.

---

1. Addresses outside this range are available for machines which need static addresses. Those machines can then be listed in the DNS configuration (*DNS Server Configuration*, page 99).

Slave DNS Server

Setup your machine as the slave server of another, master, DNS server. Just supply the IP address of the master server for the slave to mirror. Then clients can be configured to query both servers: if the master fails, the slave takes over.

Add Host in DNS

If your machine is a master DNS server, you'll be able to declare all the machines with static addresses on your network so that the DNS server can answer requests about them.

Remove Host in DNS

This is used to remove a DNS entry previously added with Add Host in DNS.

Note: Both the Add Host in DNS and Remove Host in DNS wizards only work if your machine is set up as a master DNS server.

9.4. Mail Server Configuration

SMTP stands for "Simple Mail Transfer Protocol". An SMTP server allows you to send internal and external mail through it. If your server is referenced on the Internet public DNS as an MX server for your domain name, then it also receives and manages mail from the Internet addressed to users of your domain. This wizard allows you to setup a mail server with Postfix.

Warning

Your server network parameters must not be provided by DHCP for Postfix to work properly.

The first step consists of choosing whether you intend to use an external SMTP relay or not. If you can use one provided by your ISP then choose Relay mail server in the drop-down list. Otherwise, choose Main mail server. In the procedure below only the second step differs from one configuration to the other.

1. Global Postfix Configuration

   Smtpd banner

   The banner your server advertises when talking to other servers or clients.

   Hostname

   The FQDN name of your server.

   Domain

   The domain handled by this mail server.

   Origin

   The domain name that locally-posted mail appears to come from, and that locally posted mail is delivered to.

2. Relay (for Relay mail server only)

   Relay host

   This is where you define the mail server responsible for relaying your outgoing messages.

Relay domains

> What destination domains (and subdomains thereof) this system relays mail to. Mails sent to a domain other than the local domain that are not part of the relay domains are rejected (to prevent spam).

3. Main server Configuration (for Main mail server only)

helo required

> For security reasons you might require remote clients to identify themselves before starting communication. Choose yes in this case.

Disable verify command

> The `verify` command can be used by a client to verify a specific user is actually handled by a mail server. You can disable it to prevent email harvesting by spammers.

Masquerade domains

> This field is used to masquerade the domain from which internal mail appears to come from. For example: `foo.example.com example.com` directs Postfix to masquerade `toto@foo.example.com` to `toto@example.com`.

4. Message options

A few options affecting message handling you can leave at their default values.

Maximal queue life

> If a message cannot be delivered after this delay it is sent back as undeliverable. Expressed as a number of days prefixed by the letter `d`, for example `3d` means three days.

Message size limit

> Messages larger than this size (kilobytes) are rejected. When defining this parameter, please bear in mind that binary attachments have a bigger size than their filesize because they have to be encoded differently to be sent in a mail message.

Delay warning time

> If a message cannot be delivered, the sender will receive a warning after this number of hours.

5. Network Configuration

inet interfaces

> The network interface addresses that this mail system receives mail on. By default the server listens on all network interfaces (`all`), specify `localhost` to listen only on the local interface.

my destination

> The list of domains that are delivered via the local mail delivery transport. The SMTP server validates recipient addresses and rejects non-existent recipients.

my networks

> The list of "trusted" SMTP clients who have more privileges than "strangers". In particular, "trusted" SMTP clients are allowed to relay mail through Postfix. Specify a list of network addresses or network/netmask patterns, separated by commas and/or whitespace.

If a parameter is not clear to you, please refer to the Postfix Configuration Parameters (`http://www.postfix.org/postconf.5.html`).

9.5. Samba Server Configuration

Samba allows GNU/Linux to act as a file and/or printer server for Windows® machines. Even though this wizard can help configure primary and backup domain controllers, we will concentrate here on the most common, standalone server configuration.
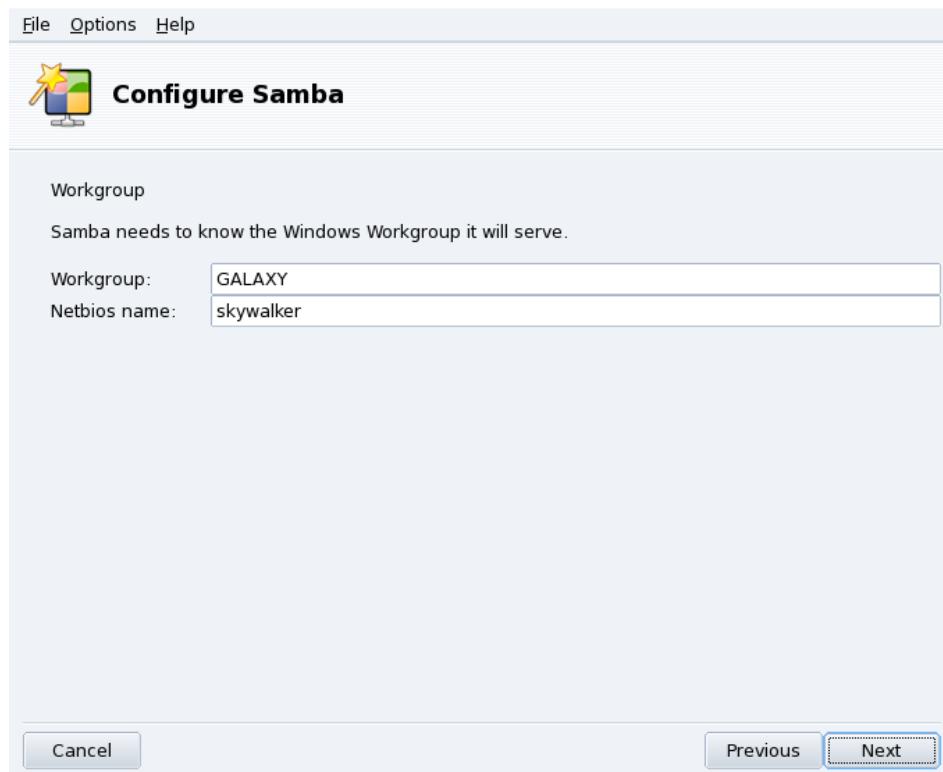
Figure 9-3. Choose the Workgroup

Enter the workgroup to be served by your Samba server and the server's NetBIOS name (figure 9-3). You can either create a new workgroup or choose an existing one, please refer to your network administrator if you are unsure.

> **Tip:** A valid NetBIOS name must follow the simple NetBIOS naming rules (basically, a 1 to 16 character mix of letters, numbers and the – sign is allowed), and be unique (ie. no other machine should have that same name) within the workgroup.
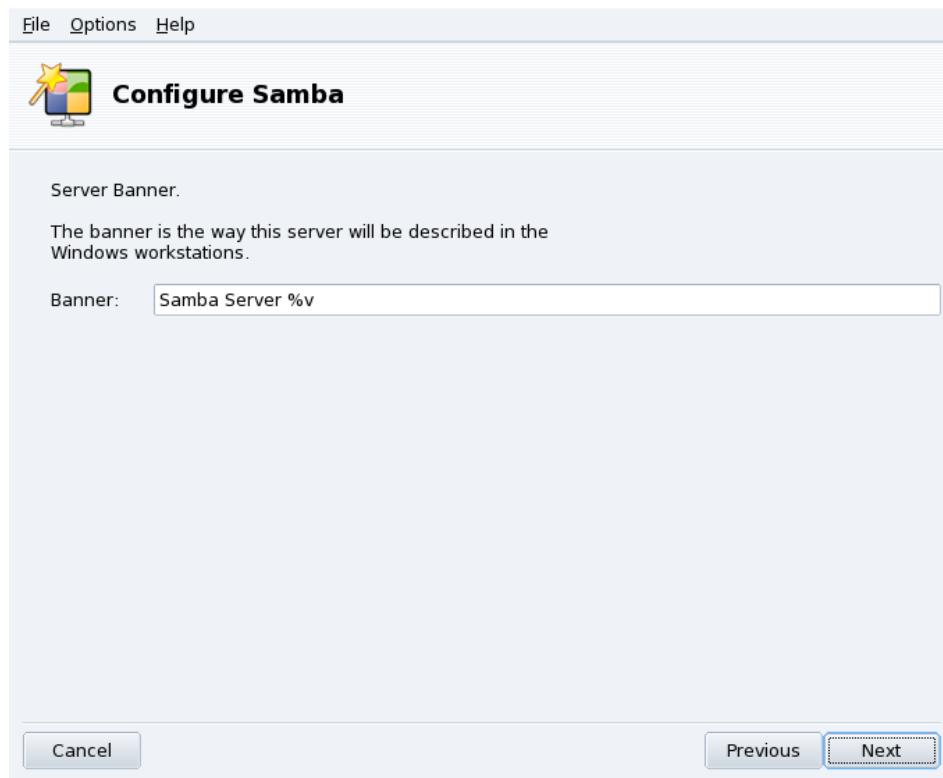
Figure 9-4. Server Banner

Then you have to specify a descriptive name for your Mandriva Linux server, as shown in figure 9-4. This is the description Windows® machines on your network get when requesting more information about the server. You may just accept the default or choose whatever name you want.

Finally you can adjust the log facility parameters. Keep the defaults unless you have specific needs.

When the Samba server is configured you can use the Samba share wizard to create new shares and manage existing ones. Please note that it is only available in Expert Mode.
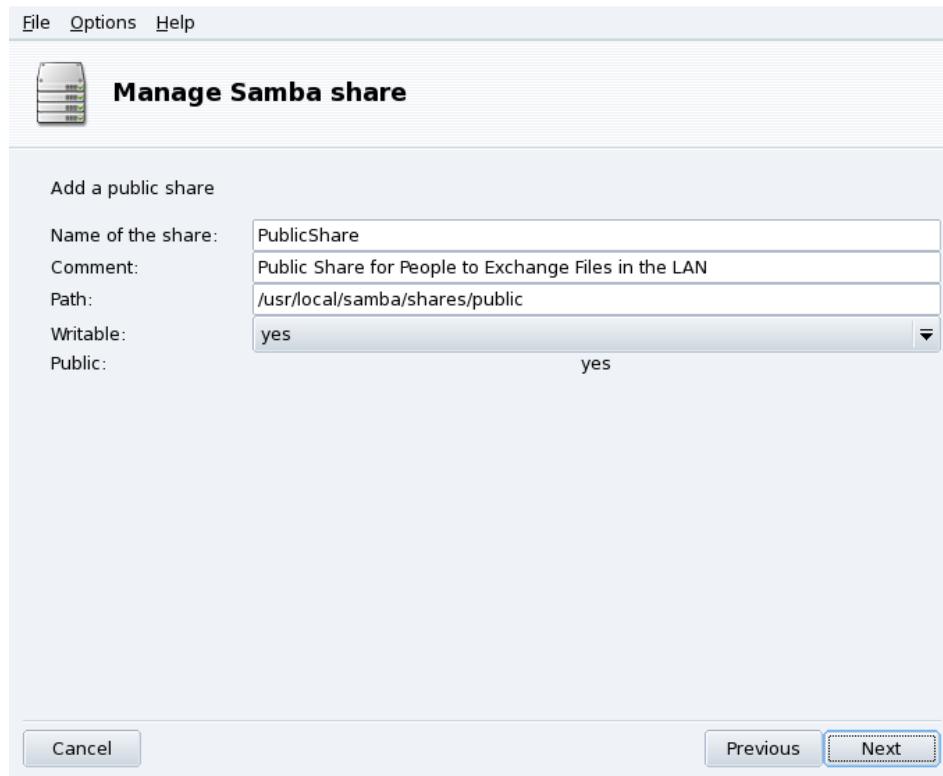
Figure 9-5. Samba Public Share Setup

Run the Samba share manager, select Public share and proceed to the next step. figure 9-5 shows an example of a public share, writable by everyone with files hosted on the `/usr/local/samba/shares/public` folder in the server.

Warning

Home directories should not be shared by means of a writable public share, use the Special share (CDrom, Homes, Profiles) option to share home directories instead.

9.6. Web Server Configuration

This wizard will simply let you specify if your web server will be disabled, visible from the local network, from the external network (generally the Internet) or from both. Check the appropriate boxes as shown in figure 9-6.

Figure 9-6. Defining the Web Server Visibility

Warning
If your server network parameters are provided by DHCP the web server might not function properly if set to be visible from the Internet.
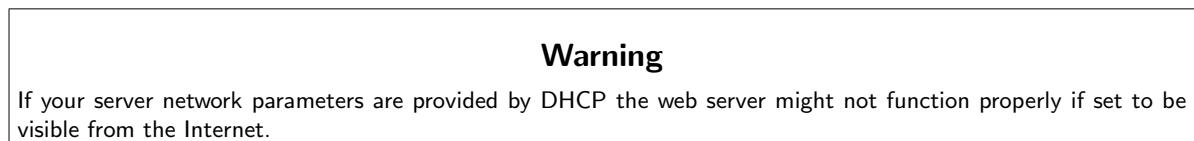
Then you can enable the feature which gives users the option to maintain their own web sites, available from the `http://server_name/~user/` URL. The directory where they store their sites (`public_html`, inside the user's home directory, by default) can also be changed if this option is checked.

Finally you can specify the directory where the files to be served by the server will be stored, known as the **Document Root**. To publish your web site, simply put the files in the chosen directory. You can connect to your web site as soon as the wizard is finished through the `http://localhost/` URL.

9.7. FTP Server Configuration

 This wizard resembles the one used to configure a web server: It will let you specify whether FTP should be disabled, visible from the local network, from the external network, or both. Check the appropriate boxes as shown in figure 9-7.

Figure 9-7. Defining FTP Server Visibility

> **Warning**
>
> If your server network parameters are provided by DHCP the FTP server might not function properly if set to be visible from the Internet.
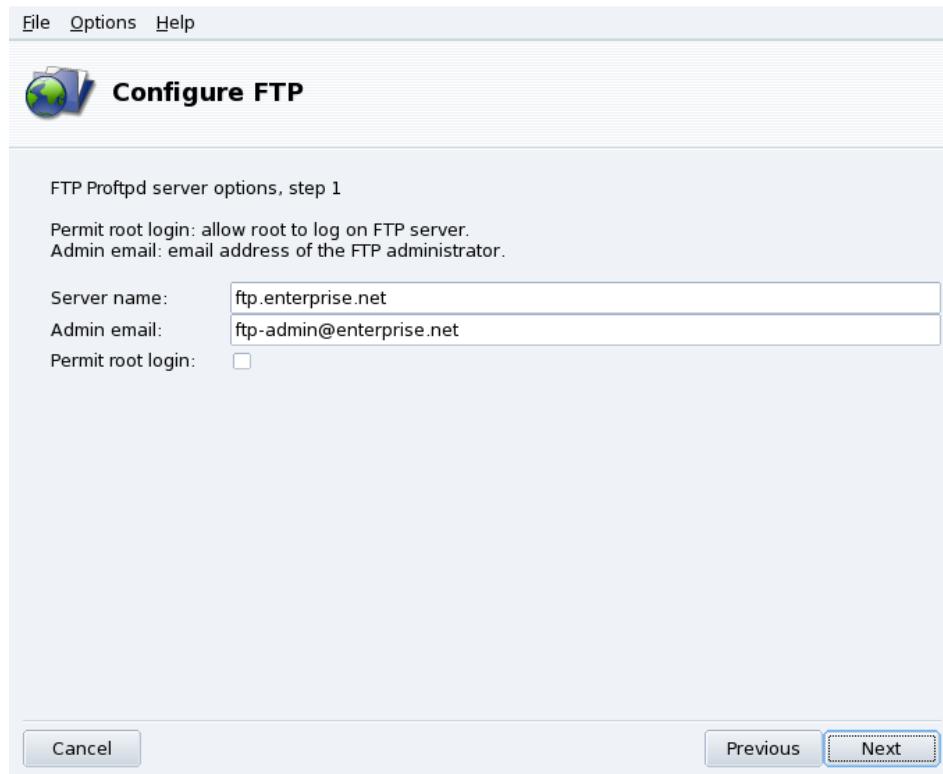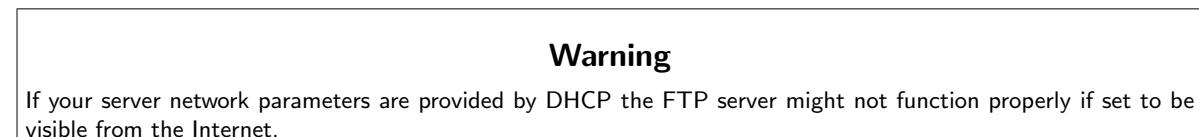
Figure 9-8. FTP Server Configuration

The basic FTP server configuration is shown in figure 9-8. Besides the server's name you should provide an email address for the administrator so that he can receive alert messages.

Admin e-mail

> Enter the address to which messages regarding the FTP server should be sent.

Permit root login

> Check this box if you wish the root user to be allowed to login into the FTP server. If the FTP authentication is made in clear text, this option is **not** recommended.

Figure 9-9. FTP Server Options

You are then allowed to configure a few options (figure 9-9):

FTP Port

> The standard FTP port is `21`, if you specify something else here FTP clients will have to be configured accordingly.

Chroot home user

> By checking this option, users who log into the FTP server will be "boxed inside" their home directories.

Allow FTP resume

> If your server is likely to host large files, it might be prudent to allow users to resume downloads.

Allow FXP

> Check this option if you want your server to be able to exchange files with other FTP servers. Please note that the FXP protocol is not very secure.

To begin populating your FTP server, simply put the files in the `/var/ftp/pub/` directory. You can connect to your FTP server as soon as the wizard is finished through the `ftp://localhost/pub` URL. Home directories are also accessible by default with local password authentication. If `queen` wants to access her home directory she has to use the `ftp://queen@localhost` URL.

> **Note:** To enable anonymous login on the FTP server, you need to install the proftpd-anonymous package.

9.8. Installation Server Wizard

You are performing lots of installations and are tired of changing CDs? This wizard is for you. It configures your machine to act as an installation server, so new machines can get all required packages directly from your server on the local network, either for initial installation or for maintenance.
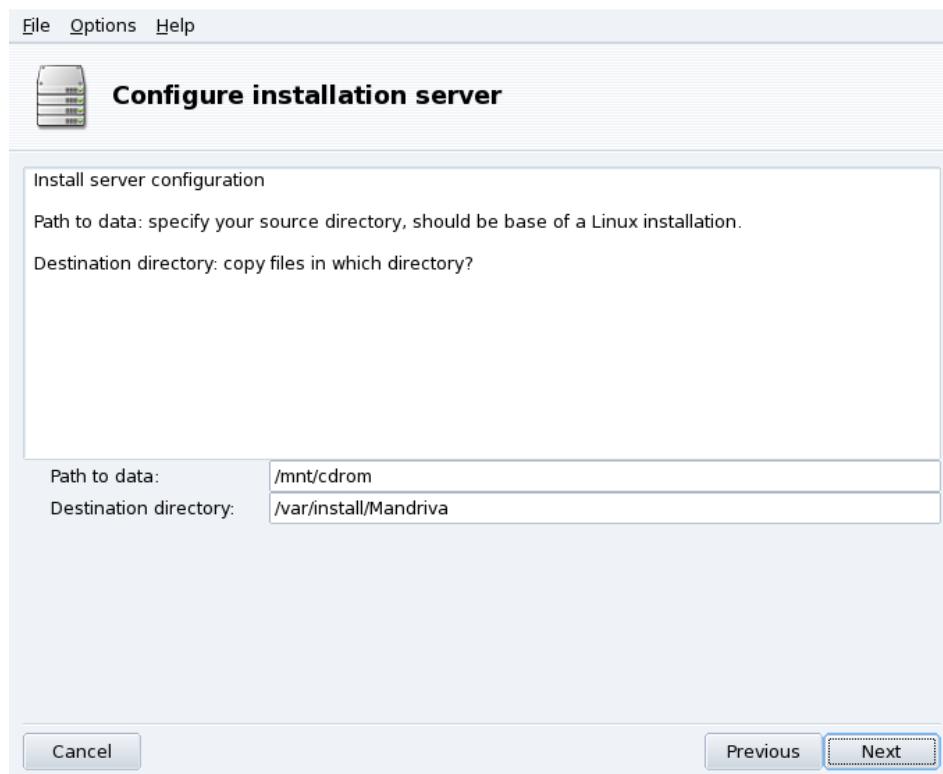
Figure 9-10. Copying Installation Sources

Specify the location to copy the CDs or DVD from, and a place on your disk where the files are to be stored.

> **Note:** If you get an error, please check that the medium you selected as source is mounted.

9.9. NIS and Autofs Servers Wizard

NIS stands for "Network Information Service" and allows you to centralize your users' authentication and home directories. Run this wizard if you want users to have access to their own environment no matter which machine on the local network they connect from.
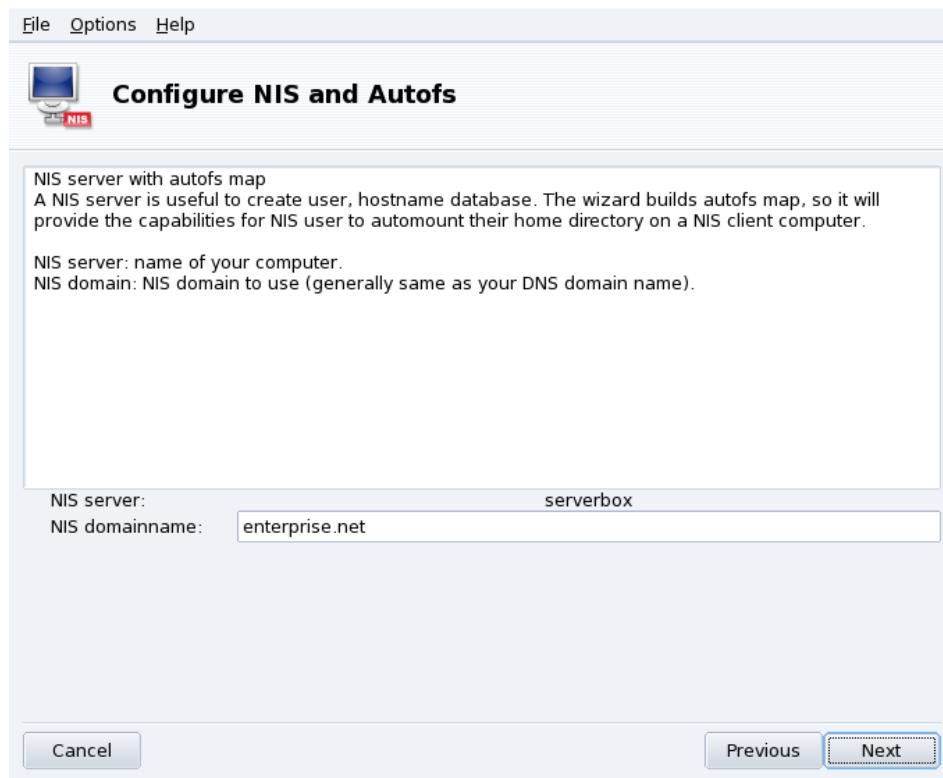
Figure 9-11. Setting NIS Server Parameters

Fill the NIS domain field with your domain name, then fill the directory to "host" the NIS users homes. When configuration is done, NIS users can login from any machine on the network that is setup to connect on your NIS server. Additionally, those users have their home directories automatically mounted locally.

9.10. LDAP Configuration Wizard

LDAP stands for "Lightweight Directory Access Protocol" and can be used to centralize directory-like information, for example address books, user account details, etc. This simple wizard allows you to setup a basic LDAP server, and add users to it. This is useful to quickly setup a LDAP-based authentication mechanism.

When you first run the wizard, you are presented with the server configuration dialog.
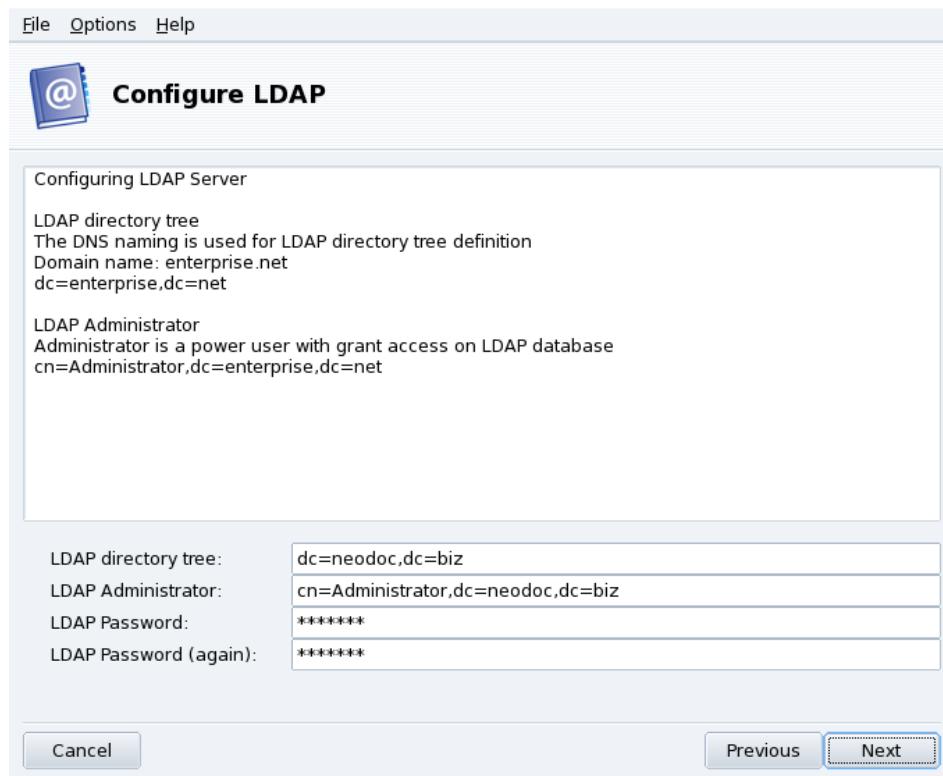
Figure 9-12. LDAP Server Configuration

Once the configuration is set and the server launched, running the wizard again gives you the following options:

Show Ldap configuration

> Shows current server configuration, useful to configure possible LDAP clients.

Delete Ldap configuration

> Removes current server configuration and stops the server. You are informed of the file name where current LDAP directory information will be stored in LDIF format.

Add user in Ldap server

> Starts a little wizard which allows you to add new users inside the users directory.

9.11. Proxy Server Configuration

A proxy server is very useful for a local network accessing many web pages across a slow, or relatively slow, connection. It maintains a cache of most visited pages so that they don't need to be retrieved again from the Internet if requested by different users. This wizards sets up the Squid proxy server.

First of all you need to choose a port for the proxy to listen to requests on. Users have to configure their web browsers to use this port as the proxy port and your server's name or IP address as the proxy server.
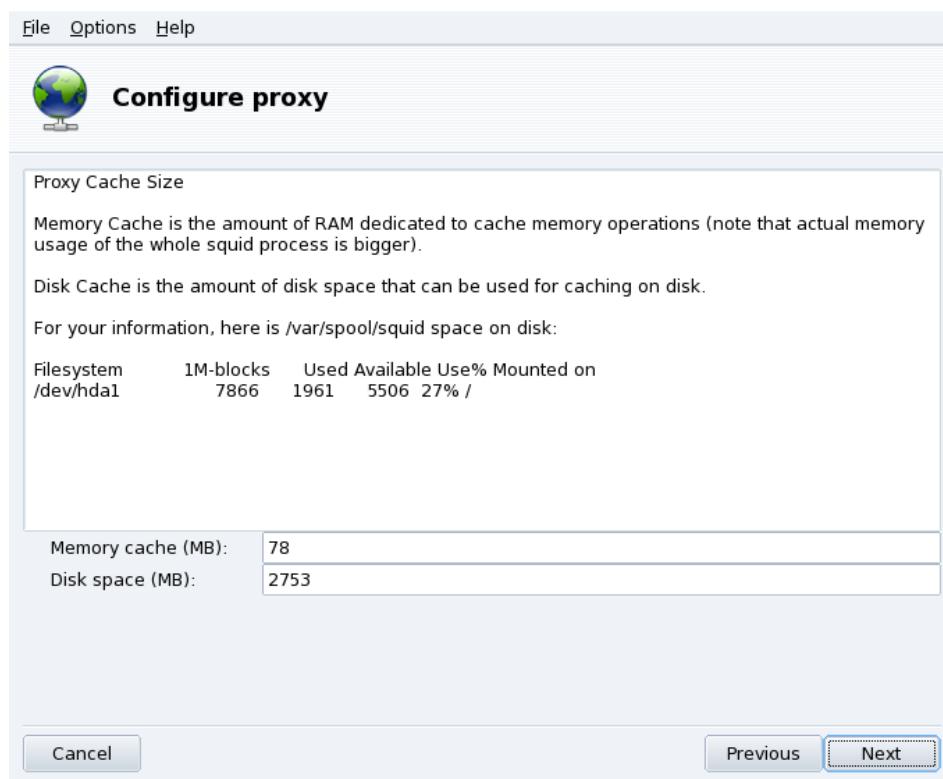
Figure 9-13. Choose the Cache Size

Depending on your machine's available memory, you can allocate more or less to the proxy. The bigger the memory cache, the fewer disk accesses on the server. Depending on your available disk size you can allocate more or less room for cached pages. The more the space, the less accesses to the Internet. The wizard chooses appropriate values for your system, if in doubt just accept the proposed ones.

In the next step, some access levels are available for clients wishing to use the proxy:

- **All.** There is no restriction, all computers are granted access to the cache. This setting is not very secure and thus not recommended.

- **Localhost.** Only the local machine, the server, can access its own proxy.

- **Local Network.** Only machines on the local network can access the proxy. This is the recommended setting.
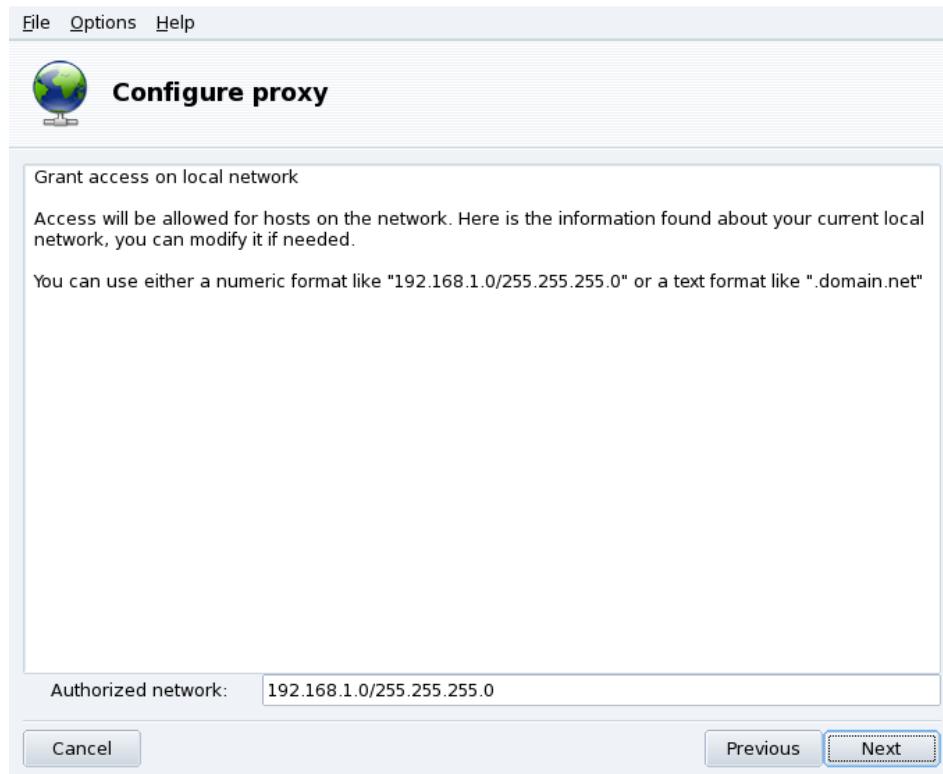
Figure 9-14. Restrict Access to a Particular Sub-network

If you have previously chosen the Local Network access policy, you can choose to restrict even more the access to a particular subnetwork or domain. The wizard will detect your LAN's network address and will offer it by default: make modifications if needed.

Finally, if your server itself has access to another larger proxy connected to the Internet, you can choose to Define an upper level proxy to which requests will be forwarded. If so, the next step will ask you for the name and port of that server.

9.12. Time Configuration

NTP stands for "Network Time Protocol" and is used to synchronize system time with reference time servers on the Internet. This wizard lets you set up a time server for your internal network. When you have set up the external time servers your own server will use to correct its internal clock, machines on your local network will be able to get the correct time from your local server.
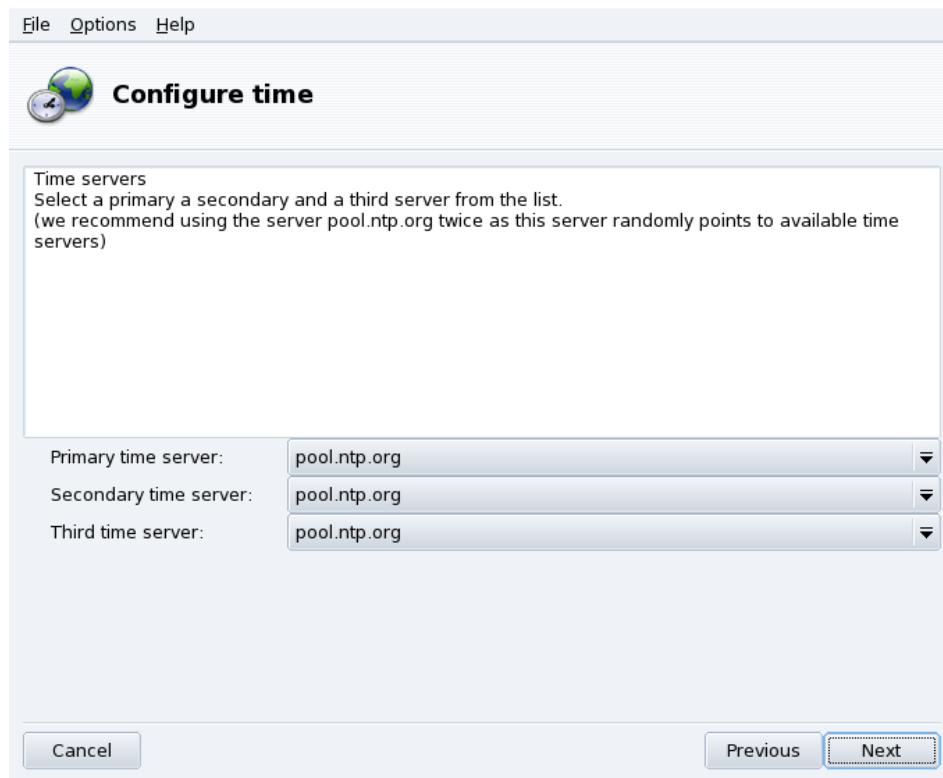
Figure 9-15. Choosing your Time Servers

Choose the time servers to query, in order of preference. It is advisable to keep the default suggested ones, otherwise choose servers which are geographically close to you. Then the time zone has to be set, use the pulldown lists to choose your geographic location.

Index